中小企業向けサイバーセキュリティ事後対応支援実証事業
(地域名：宮城県、岩手県、福島県)

成果報告書

請負事業者：株式会社デジタルハーツ

目次

１．背景・目的

IoT や AI といった技術により実現される「Society5.0」「Connected Industries」では、サイバー空間とフィジカル空間が密接に関わることにより、サイバー攻撃がフィジカル空間へ及ぼす影響が大きくなる。また、「Connected Industries」を始めとするネットワーク化の進展は、企業間のつながりなど様々な形のつながりを生むため、悪意のある者にとって新たな攻撃の機会となるおそれがある。

さらに、攻撃の手法も進化しており、サイバー攻撃の脅威はあらゆる産業活動に潜むようになっている。例えば、スマートフォンのファームウェアに、ユーザーの個人情報等を国外に送信する機能が埋め込まれる等、製品やサービスを製造し流通する過程で不正なプログラムの組み込みや改造が行われるサプライチェーンリスクの問題も顕在化しつつある。サイバーセキュリティ対策を理由として、サプライチェーンへ参加できなくなる中小企業が多数生まれることは、多くの中小企業の経営を苦しめるだけでなく、我が国の産業競争力全体にとって大きな影響を与えることになるため、中小企業のサイバーセキュリティ対策支援を進めることは喫緊の課題である。

一方、多くの中小企業はサイバーセキュリティに対する意識が低く、自社がサイバー攻撃に遭うと思っていないため、サイバー攻撃に遭っていること自体に気付かず、その結果、サイバー攻撃の被害が拡大するケースも多く発生している。また、多くの中小企業は IT やサイバーセキュリティに関する知識が乏しく、IT に関するトラブルが発生した際にシステムの不具合が原因なのか、サイバー攻撃が原因であるか自社で判断することは困難である。

このような実態から、困ったときに気軽に相談できる窓口や、サイバー攻撃に遭った際に事後対応をするサービスに対するニーズはあるが、サービス提供側が、中小企業の被害実態や、中小企業支援に必要な人材スキル等の把握ができていないため、現状は中小企業のニーズに合った製品、サービスが提供されてない。そのため、中小企業の被害実態等を把握することで、中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らかにし、中小企業の支援機能を低コストで構築することで、中小企業のセキュリティ対策強化を図る必要がある。

こうした背景の下、本事業の実施を通じて、中小企業におけるサイバーセキュリティの意識向上を図るとともに、中小企業の実態に合ったサイバーセキュリティ対策を定着させていくことを本事業の目的とする。

2．事業概要

2-1．事業概要

上記の背景・目的を踏まえ、株式会社デジタルハーツ（以下「デジタルハーツ」という。）は、以下の３つの基本コンセプトに沿って「中小企業サイバーセキュリティお助け隊事業 in 東北」（以下「本実証事業」という。）を実施した。実施にあたっては、損害保険ジャパン日本興亜株式会社（以下「損保ジャパン」という。）の協力を得た。本実証事業の対象は、以下に示す考え方に基づき、仙台市を中心とした宮城県を中心に、福島県及び岩手県を含めた東北地域の一部（以下「実証地域」という。）における中小企業とした。

（１）サイバーインシデント実態の可視化

中小企業に対するサイバーセキュリティ対策は喫緊の課題であるが、サイバー攻撃を受けているという被害の自覚がない場合が多く、自らコストをかけて対策に取組むインセンティブが低い状況にある。一方で、サプライチェーン上でサイバーインシデントが発生することにより、大きな被害が生じるリスクが発生している。例えば、2019 年 3 月 29 日には、東京都内の販売・物流会社のネットワークへの不正アクセスが行われたことで、大手自動車会社が有する約 310 万人の顧客情報が流出する事件があった。

東北地域は、首都圏や名古屋、大阪といった主要都市と比較すると経済圏としては小さいものの、自動車産業や電子部品産業などにおけるサプライチェーン上の重要な位置づけを占めている。サイバー攻撃はサプライチェーン上の脆弱な組織が攻撃対象となりやすいことを踏まえれば、東北地域の中小企業におけるサイバーインシデントの実態把握を軽視することはできない。

本実証事業では、実証地域内の中小企業にネットワークセンサーを設置することでサイバー攻撃の実態を可視化し、多くの中小企業が抱える漠然とした不安を対策可能な課題として整理することに取り組んだ。今回設置したセンサー「Starlight」は、サイバーインシデントの判定に必要なパケット情報を幅広くかつ効率的に収集することに加え、収集した通信ログを各種セキュリティ機能で分析し、独自の AI で危険度を自動判定することができるため、従来のセキュリティ監視装置に比べて正確にサイバーインシデントを把握することができるのみならず、設置対象企業に専門的な知識を要求しないため、中小企業に対しても容易に導入することが可能となっている。

これにより、サイバーインシデント実態を可視化し、サイバー対策は中小企業経営における必要不可欠な投資であるという認識を浸透させることを目指した。

（２）地域内のサイバー対策強化

多くの中小企業には IT の専門的知識を有する人材が不足しており、経営者が自らネットワーク構築・運用業務を行っているケースも多い。こうした場合、IT に関するトラブルが発生した場合にサイバー攻撃が原因か否かの判定が難しく、思い切った IT 活用に踏み切ることができない原因にもなっていると考えられる。

特に、東北地域は首都圏からの地理的アクセスもよく、東日本大震災からの復興も今なお国家的に重要な課題であるところ、IT 活用を進めていくことでさらなる経済成長が見込まれることから、デジタル化は喫緊の課題である。一方で、十分かつきめ細かな情報が提供されていないことから、IT 導入補助金の利用実績も少なく、IT 活用やサイバー対策に踏み切れていない現状がある。

このため、実証地域内のサイバーインシデントに関する情報を一元的に集約し、地域内の中小企業にとって分かりやすい情報に加工して発信するポータルサイトの設立・運営を通じて、困ったときに相談できる窓口や、サイバー攻撃にあった際に事後対応を受けられやすい環境を構築した。これにより、実証地域内のサイバー対策強化を面的に図ることを目指した。

（３）中小企業向けサイバーセキュリティ対策の事業化

中小企業向けにサイバーインシデントか否かを相談する窓口や、サイバー攻撃に遭った際に事後対応をするサービスに対するニーズは十分考えられるものの、被害実態や中小企業支援に必要な人材スキル等の把握ができていないため、現状は中小企業のニーズに合ったサービスが提供されていない。民間企業の視点からはどうしても規模の経済が働く大都市圏を中心にサービス提供が検討されがちである一方で、サイバー攻撃はサプライチェーン上の脆弱な組織から狙われる可能性があることを踏まえれば、こうした規模の経済が働きづらい地方において優先的に公費による実証を行いサービス検討に必要な情報を収集すべきである。

こうした現状を踏まえ、本実証事業の成果を公表することにより、IT ベンダーや損害保険会社などがサービス提供を行いやすいオープンな環境を構築し、中小企業の実態に合ったサイバーセキュリティ対策の定着を目指した。デジタルハーツは、中小企業向け IT サポートやサイバーセキュリティ対策事業を行っており、本実証の成果を踏まえた自主事業化を検討している。加えて、実証結果を損保ジャパンに共有し、あるべきサイバー保険の姿についての検討を行うこととした。

また、今回の実証を通じて協力を得た官公庁・外郭団体・経済団体等に呼びかけることで、実証地域のサイバーセキュリティに関する団体の活動を活性化し、今後も継続的にサイバーセキュリティに関する各種活動を行うための基盤を構築することを目指した。

2-2. 支援体制

2-2-1. 支援体制概要

以下の機能を備えた中小企業向けサイバーセキュリティ事後対応支援体制を構築した。(図 1)

（１）中小企業からの相談受付及び対応（情報ポータル・支援チーム）

（２）相談内容がサイバーインシデント等であるかの判断（実証用機器・監視チーム）

（３）サイバーインシデント等が発生した場合の支援の提供（監視チーム・支援チーム）等

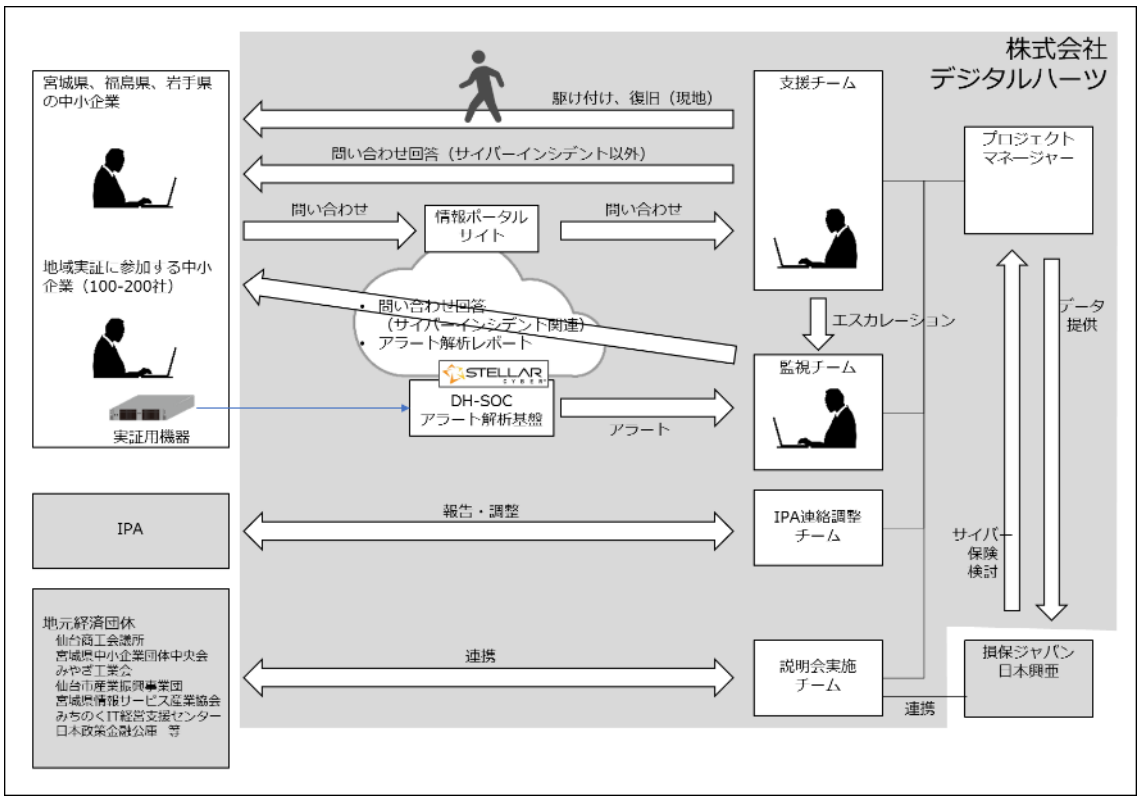


図１.支援体制図

なお、支援チームのプロジェクトリーダーには情報処理安全確保支援士を選任した。

２-２-２. 支援機能

以下のサイバーセキュリティ事後対応支援を提供することとした。

- 中小企業からの相談受付及び対応

情報ポータルサイト上に、実証期間中（2019 年 7 月 1 日から 2020 年 1 月３１日まで）、サイバーインシデント問合せフォームを設置して実証地域内の中小企業からの相談を受け付けた。ポータルサイトからの相談受付は 24 時間提供した。

- 相談内容がサイバーインシデント等であるかの判断

デジタルハーツは受け付けた問合せの内容を確認し、サイバーインシデント等であるかの判断を行った。判断が難しい場合は、地域実証への参加を誘導し、Starlight を設置して通信ログを取得し、当該ログに基づき、サイバーインシデント等であるかの判断を行った。サイバーインシデントの判定は、デジタルハーツの営業日 9 時～17 時のみ提供することとした。

- サイバーインシデント等が発生した場合の支援の提供

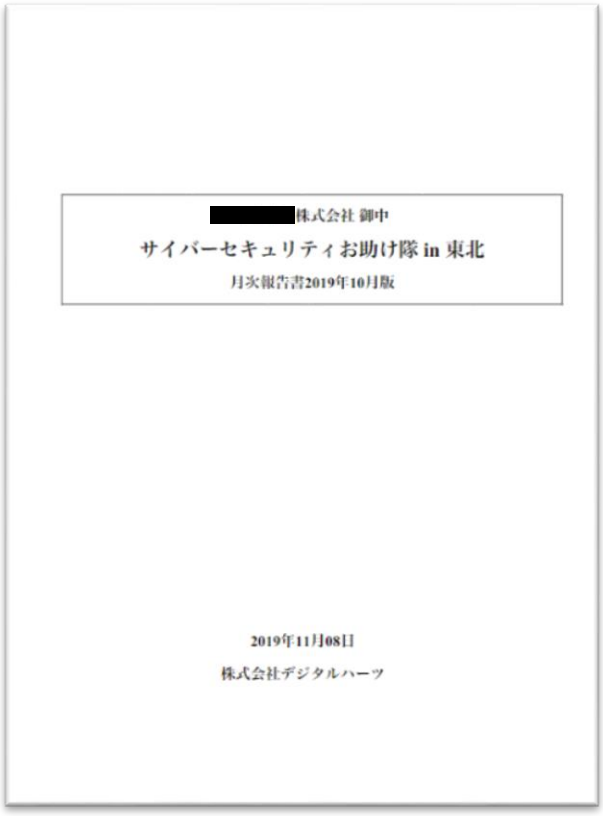
問合せまたは Starlight からのアラートにより、サイバーインシデント等が発生した場合には、デジタルハーツから必要な対応方法を提示することとした。復旧支援は地域実証に参加している企業に限定して行うこととし、問合せフォーム経由で連絡があった者に対しては実証参加への誘導を行うこととした。

なお、Starlight によるアラートは 24 時間提供するが、復旧支援はデジタルハーツの営業日 9 時～17 時に提供することとし、復旧支援は基本的に翌営業日以降の対応とした。

- 実証状況の提供

中間報告会及び成果報告会にて、実際に発生したインシデントの事例についての紹介や、アラート発生の統計情報の提供を行った。

またネットワークセンサーを設置した企業に対しては、月次報告書を送付して実証参加企業のインシデントアラート状況や通信状況の情報提供を行った。(図 2,図 3)



[redacted]株式会社 御中

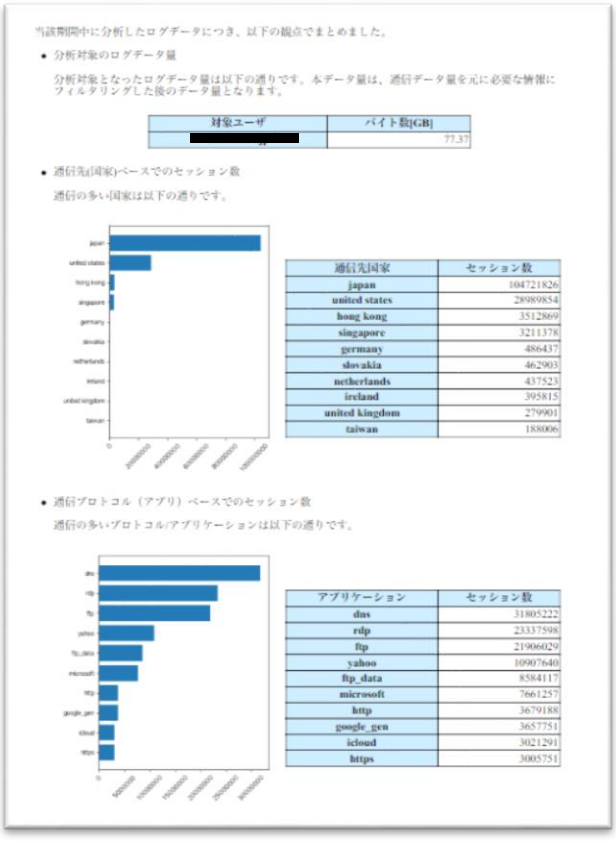
サイバーセキュリティお助け隊 in 東北

月次報告書2019年10月版

2019年11月08日

株式会社デジタルハーツ

図 2.月次報告書サンプル 1



当該期間中に分析したログデータにつき、以下の観点でまとめました。

- 分析対象のログデータ量

分析対象となったログデータ量は以下の通りです。本データ量は、通信データ量を元に必要な情報にフィルタリングした後のデータ量となります。

対象ユーザ	バイト数[GB]
[redacted]	77.37

- 通信先(国家)ベースでのセッション数

通信の多い国家は以下の通りです。

通信先国家	セッション数
japan	104721826
united states	28989854
hong kong	3512869
singapore	3211378
germany	486437
slovakia	462903
netherlands	437523
ireland	395815
united kingdom	279901
taiwan	188006

- 通信プロトコル（アプリ）ベースでのセッション数

通信の多いプロトコル/アプリケーションは以下の通りです。

アプリケーション	セッション数
dns	31805222
rdp	23337598
ftp	21906029
yahoo	10907640
ftp_data	8584117
microsoft	7661257
http	3679188
google_gen	3657751
icloud	3021291
https	3005751

図 3.月次報告書サンプル 2

2-3. 監視サービスの概要

2-3-1. 監視サービスの設計

対象となる企業が中小企業ということから、以下のような方針で当事業のサービスを設計した。

- 監視ターゲット
  多くの中小企業では外部ネットワークへの公開サーバ（メールサーバや Web サーバなど）は社内に設置しておらず、社内 PC からインターネットのアクセスのみにネットワークを利用していると考え、主な監視対象を外部からのネットワーク攻撃ではなくマルウェアなどの侵入や侵入したマルウェアの外部との通信とすることとした。

- 新規に監視機器を設置する
  対象となる中小企業にはどのようなネットワークセキュリティ機器（UTM や FW など）が設置されているか不明であり、かつ高価で高機能な UTM などはほとんど設置されていないと考え、新規に監視用の機器を設置することとした。

- ネットワーク環境を変更しない
  ほとんどの中小企業では IT やネットワークの専任の管理者が不在であり、社内ネットワークの構成なども把握されていないと考え、なるべく既存のネットワーク構成を変更しないで導入できるような構成にすることとした。

2-3-2. 監視サービス内容

前項での検討した設計方針を基に、Stellar Cyber 社のセキュリティ監視システム「Starlight」を利用した監視サービスを提供した。

当初想定した典型的な構成要素例は以下のとおりである(図 4)。

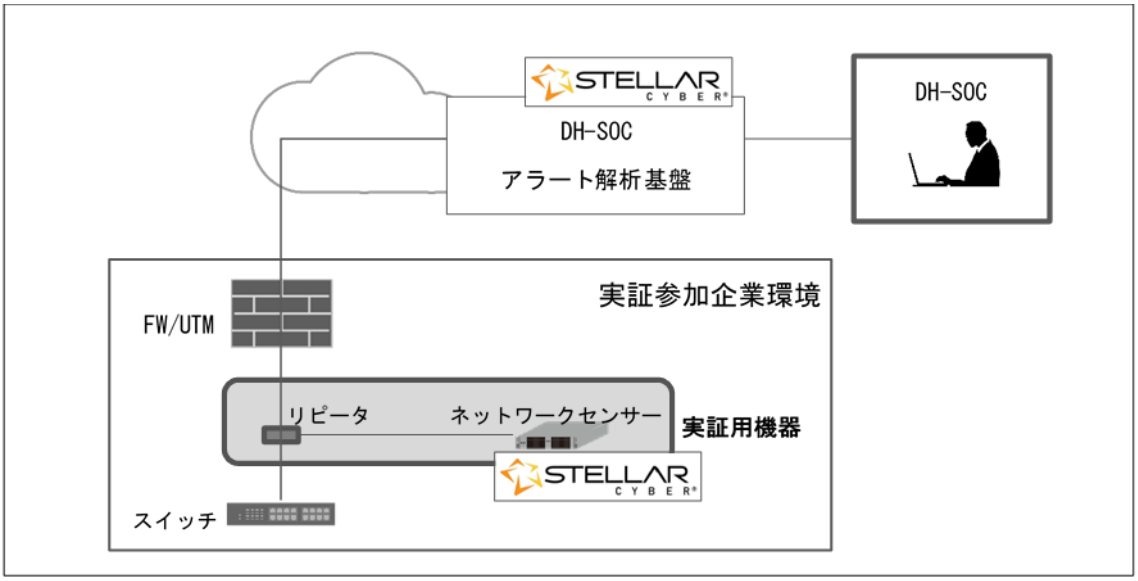


図 4.監視サービス構成例

- Starlight ネットワークセンサー
  ネットワークのトラフィック情報を収集して効率的にアラート解析基盤に送信する監視装置。トラフィック情報に加え、特定のパケットやネットワーク上を流れるファイルもアラート解析基盤に送付して分析で利用することができる。また、ネットワークセンサー単体でも Port Scan や SYN flood、DNS Tunneling などの不正なアクセスを検知してアラート解析基盤に通知することもできる。

- アラート解析基盤
  実証参加企業に設置したネットワークセンサーからのデータを集めて分析するサーバ装置。IDS や Sandbox の機能も備えており、ネットワークセンサーから送られてきたパケットやファイルを集中的に分析することができる。
  アラート解析基盤では、トラフィック情報や IDS/Sandbox からのデータを自動的に相関分析し、さらに AI を使って危険度を判定し、危険度が高い事象についてはアラートを発する。

- DH-SOC デジタルハーツの監視員がアラート解析基盤の内容を確認・分析し、実証参加企業にとって本当に危険な攻撃であるインシデントであるかどうかを判定する。インシデントの場合は企業の担当者に連絡し、セキュリティ対策について助言する。

実証参加企業への導入にあたり、前項に挙げた方針に合わせ以下のような工夫を行った。

- ネットワーク構成を変更しない
  Starlight のネットワーク情報を収集するネットワークセンサーは通常ネットワークスイッチや UTM/FW/ルータなどのミラーポートに接続してネットワーク上のパケットを監視するが、今回の対象企業においてミラーポート付きのネットワーク機器が導入されている企業はほとんどなかったため、別途リピータを用意し、UTM/FW/インターネットルータと社内のネットワークスイッチとの間に設置してそこを流れるパケットのコピーをネットワークセンサーで監視することとした。
  それにより、実証参加企業のネットワーク構成を変更する必要はなく、リピータ設置時の瞬断だけで簡単に設置できるような構成とした。

- メンテナンスフリー
  Starlight のネットワークセンサーはソフトウェアとして提供されるが、デジタルハーツ側で事前にファンレスの小さな Linux ボックスにインストール、設定し、実証参加企業への導入時には設置するだけで動作するようにした。それにより導入作業を短時間で行えるようにした。
  またネットワークセンサーを導入する Linux ボックスはファンレス/HDD レスとしてメンテナンスフリーで安定して動作する機器を選定した。

2-3-3. *Starlight* の特徴

本実証事業において採用した Stellar Cyber 社のセキュリティ監視システムには以下のような特徴がある。

- ALL in ONE
  Starlight には NTA（Network Traffic Analysis、ネットワーク・トラフィック解析）、IDS（Intrusion Detection System、侵入検知システム）、Sandbox（動的なマルウェア検知機能）といった各種のセキュリティ検知機能や、それらの情報を相関分析する SIEM（Security Information and Event Management、セキュリティ情報イベント管理機能）がすべて搭載されている。(図 5)
  これらの高度なセキュリティ検知機器は高価であるため中小企業で導入することは難しいが、Starlight ではすべての機能を備え、さらにマルチテナントでそれらの機能を共有することにより、中小企業でもこれらの高度なセキュリティ検知機能を利用できるようにしている。

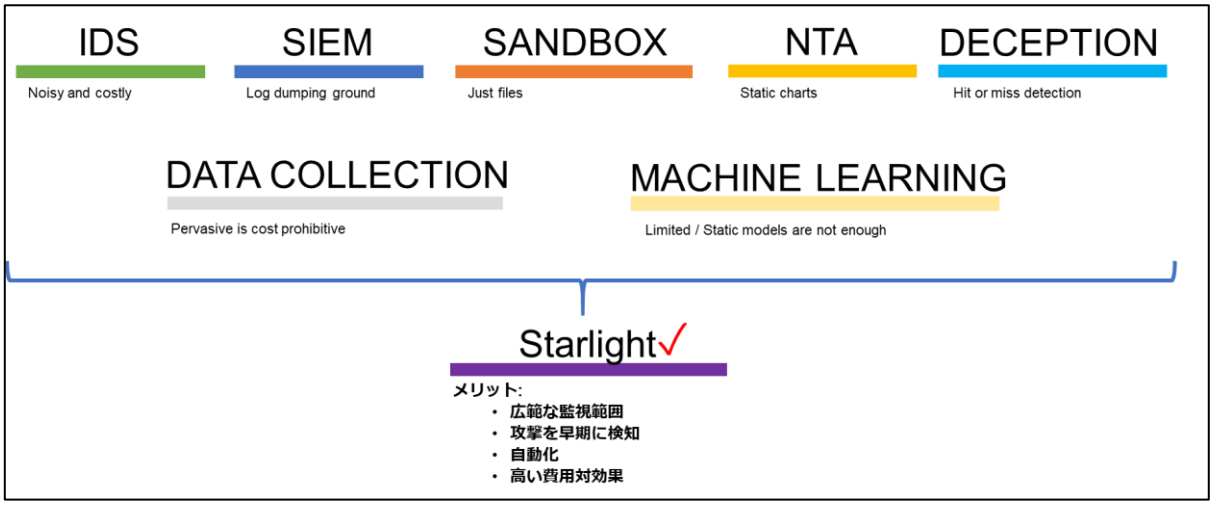


図 5.Starlight の搭載機能とメリット

- 幅広いセキュリティ検知機能

  Starlight では Cyber Kill Chain の各段階で攻撃や攻撃の兆候を幅広く検知する機能を備えている。Cyber Kill Chain とは、攻撃者によるサイバー攻撃の手順を階層化したものであり、一般的には偵察（Reconnaissance）、武器化（Weaponization）、配送（Delivery）、攻撃（Exploitation）、インストール（Installation）、遠隔操作（Command & Control）、自動実行（Exfiltration & Actions）の 7 段階に分けられる (図 6)。このうち「武器化」は攻撃者側での作業であり、攻撃を受けた側では検知できないため今回は考慮しない。

  攻撃者によるサイバー攻撃の多くはこの段階を経て最終的な目的（情報の取得や改ざん、破壊など）を遂げるため、被害が発生する前の段階で攻撃の兆候を検知しブロックすることにより、被害を抑えることができる。

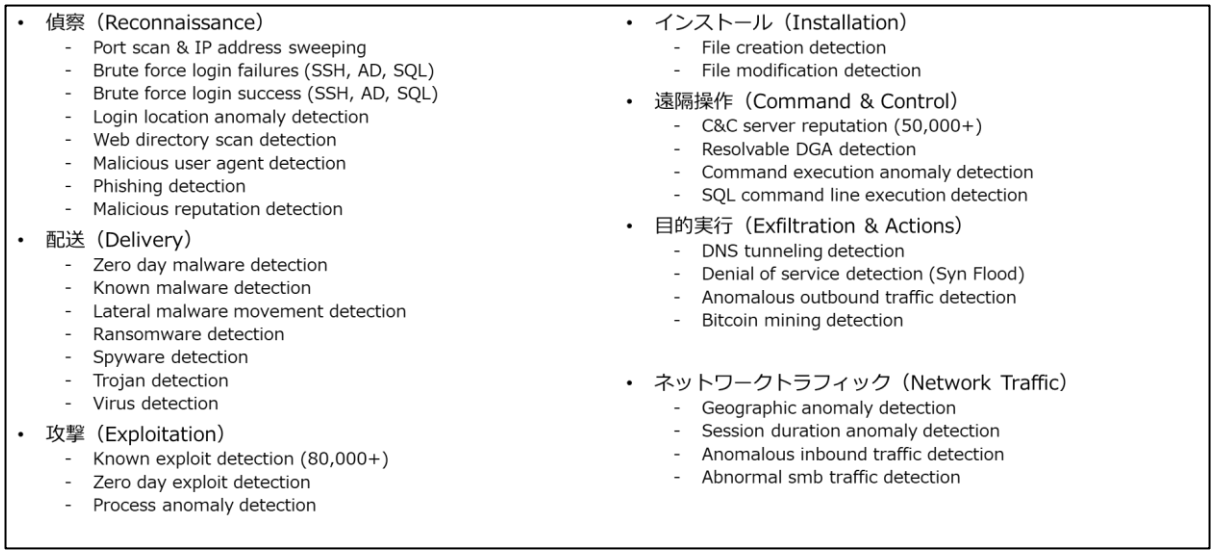


図 6.Starlight の検知項目

- 統合監視

  Starlight サーバはマルチテナントに対応している(図 7)。そのため、多数の実証参加企業に設置したネットワークセンサーからのデータを一つのサーバで統合的に監視することができるだけでなく、個々の企業のトラフィックについて個別に分析することも可能となっている。

図 7.Starlhght の監視コンソール画面例

- 効率的なデータ収集

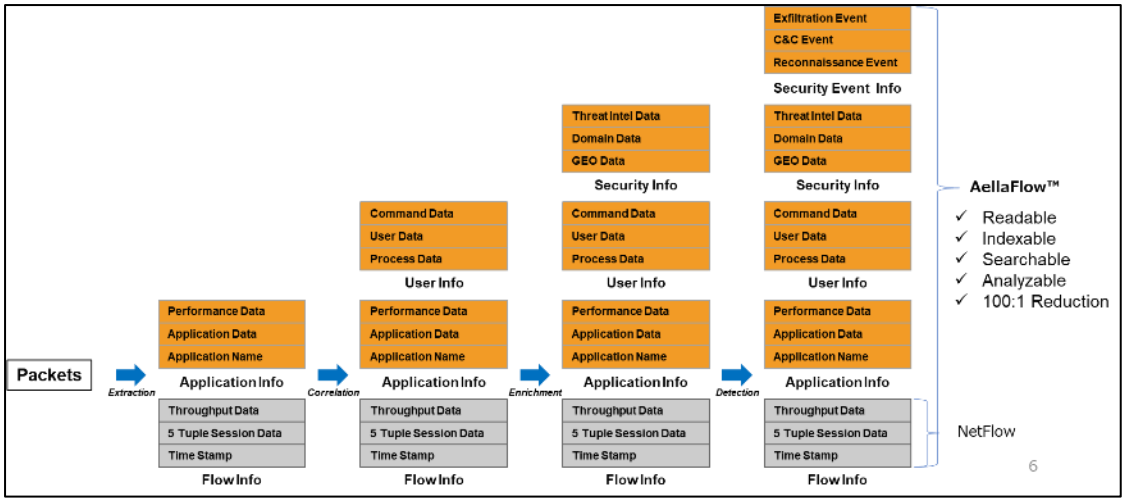


図 8.Aella Flow による効率的なデータ収集イメージ

Starlight では、監視対象ネットワークに設置したネットワークセンサーからのトラフィック情報を独自のデータ形式「Aella Flow」で効率的に収集できるようにしている(図 8)。
また「Aella Flow」は拡張可能なデータ形式であり、各種のセキュリティ検知装置からサーバに集められた相関するデータを Aella Flow に自動的に補完することで、サーバに置いて効率的に分析を可能としている。

- AI 分析

Starlight サーバには多数の AI 機能が動作している。各種のセキュリティ攻撃ごとに学習済みの AI が Aella Flow データを分析し、攻撃を検知することができる。また、各ネットワークのトラフィックを自動的に学習することにより、異常なトラフィックを検知する AI も搭載している(図 9)。
これらの AI の分析結果を基に、それぞれのトラフィックの危険度を判定することでセキュリティ攻撃を正確に検知して誤検知や過検知をなくす。また、これらの処理がすべて自動化されているため、監視員による監視作業を大幅に効率化することができる。

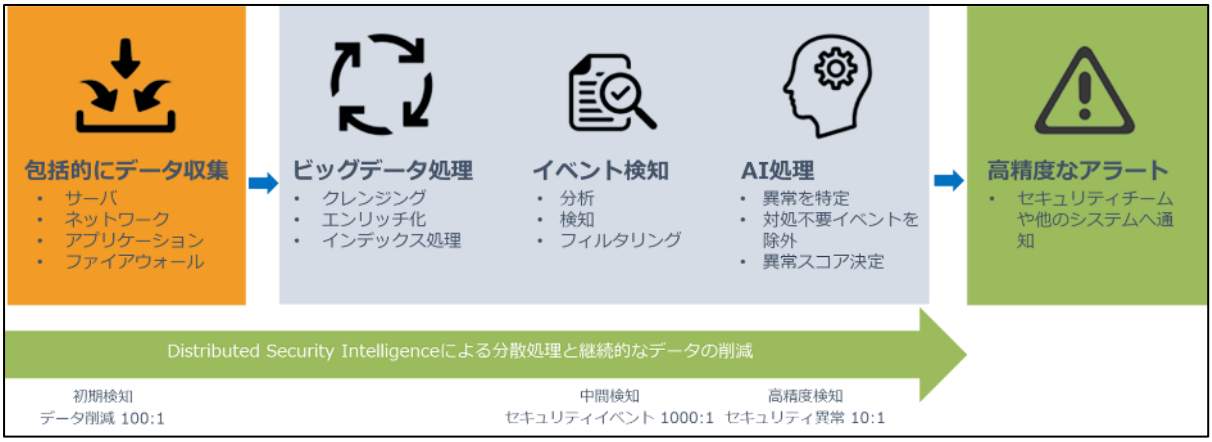


図 9.AI 分析の概要

2-3-4. 採用した監視サービスの特徴との違い

セキュリティ監視サービスの多くは、UTM（Unified Threat Management、統合脅威管理機器）の監視を行う。UTM はインターネットと社内ネットワークとの境界線に設置し、FW や IDS、アンチウィルスやアンチスパム、Web フィルタリングなどの機能を搭載した装置である。

そのため UTM ではインターネットからの多数の攻撃を検知してブロックしているが、ほとんどの監視サービスはその UTM のログからアラートを上げている。つまり、UTM で検知・ブロックした攻撃をアラートとして上げているが、その攻撃は既に UTM でブロックされていることになる。UTM で検知できていない攻撃は監視サービスでも検知できておらず、アラートとして上げられないことがほとんどである。

今回の実証事業において採用したデジタルハーツの監視サービスでは、ネットワークセンサーを UTM/FW/インターネットルータの内側（社内ネットワーク側）に設置した。それにより、UTM/FW/インターネットでブロックされた攻撃については検知しないが、UTM/FW/インターネットを通過した攻撃についてパケットやトラフィックを分析することで検知している。さらには、社内の PC からインターネットへの通信を監視・分析することにより、Web やメールを通じて社内に入り込んだマルウェアの C&C サーバとの通信などを監視・検知することを可能とした(図 10)。

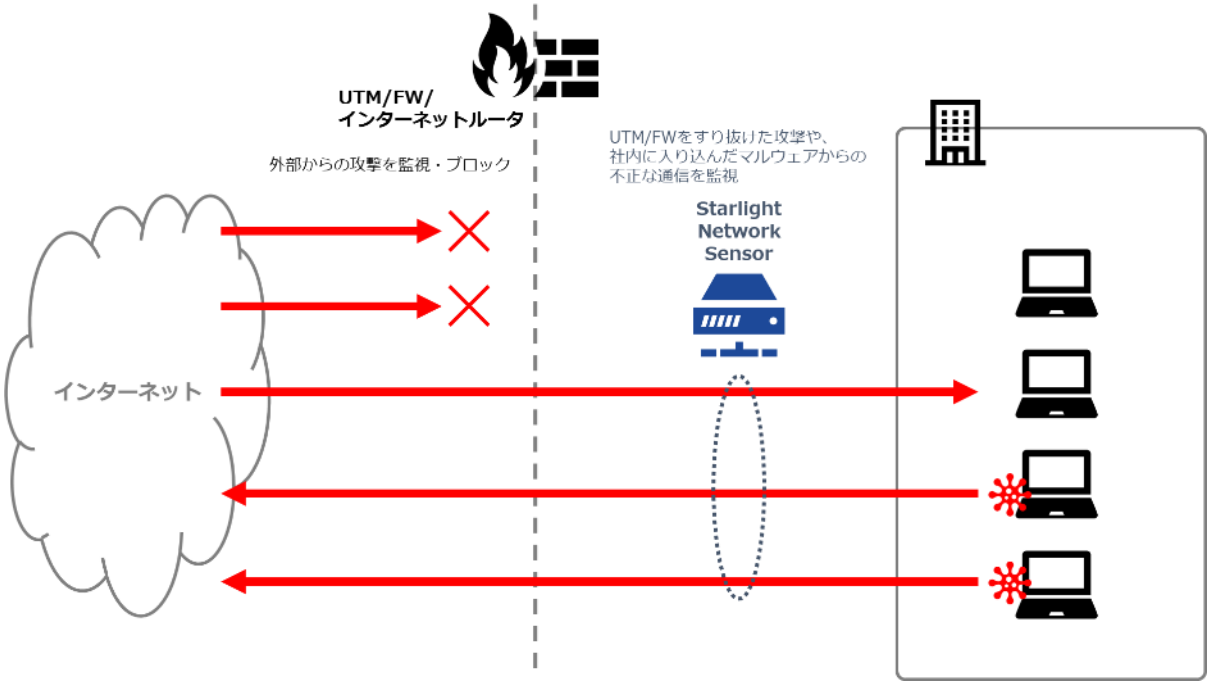


図 10.採用した監視サービスの特徴

3．事業実施結果

3-1．説明会･報告会

7 月 1 日以降、地元経済団体等への個別の説明を行い、実証参加企業の募集を行った。また、以下のとおり、事業説明会、中間報告会、及び成果報告会を実施した。

3-1-1．事業説明会

以下のとおり、事業説明会を実施した。当初、7 月 29 日（月）14:00 開始で企画し、地元経済団体のメーリングリスト等による案内によって集客を行ったが、集客が思わしくなかったため、延期として地元企業等へのヒアリングを行った。その結果、月末･月初は参加が難しい企業が多いことや、東北の人々の多くは平日の業務時間中にはこうしたセミナーには参加しない等のアドバイスを得たことを踏まえ、月の中旬の夕方に複数開催することとして、改めて企画を行った。

- 2019/9/11（水）18:00-20:00　仙台

  場所：TKP 仙台カンファレンスセンター　ホール

  参加者数：34 名（26 社）
  参加者からのフィードバック： 5 社からの実証申込み（内、機器設置できたのは 4 社）

  説明会の内容：
  「中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について」経済産業省
  「IT を活用した業務効率化について」株式会社あしたのチーム
  「実証事業の内容紹介」デジタルハーツ

  備考：
  地元経済団体等からは、単にサイバーセキュリティのみの内容とするよりも、IT の利活用などの文脈の方が関心を惹きつけられるのではないかという助言もあり、東北地域で中小企業向けに人事分野の IT 活用を普及啓発している株式会社あしたのチームに依頼し、IT 利活用の必要性や効果について説明を行ってもらった。しかし、一部の参加者からは、サイバーセキュリティのセミナーにおいてそれ以外の題材の講演に対し違和感が示された。

図 11.事業説明会風景（仙台）

- 2019/9/19（木）18:30-20:00 郡山

  場所：郡山商工会議所　会議室

  参加者数：3 名（2 社）
  参加者からのフィードバック：0 社からの実証申込み

  説明会の内容：
  「中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について」経済産業省
  「実証事業の内容紹介」デジタルハーツ

  備考：地場企業等に集客を要請して行ったが、思うように集客を行うことができなかった。

図 12.事業説明会風景（郡山）

- 2019/9/20（金）18:30-20:00 盛岡

  場所：いわて県民情報交流センター（アイーナ）

  参加者数：15 名（12 社）
  参加者からのフィードバック：2 社からの実証申込み（内、機器設置できたのは 2 社）

  説明会の内容：
  「中小企業におけるサイバーセキュリティ対策普及に向けた国等の支援事業について」経済産業省
  「実証事業の内容紹介」デジタルハーツ

  備考：
  申込みがなかった者からの飛び込み参加が複数あった（岩手の会のみであり、県民性と思われる）。Starlight のコンソール画面を用いた実際の監視業務など技術的な内容を紹介したところ、聴衆の関心を惹きつけることができた。他地域でのセミナーでの反響も踏まえ、東北地域では多数の参加者を集めることが難しいが、参加者の意識のレベルは高く、具体的・技術的な内容への関心の高さがうかがえた。全体の前で質問をする者は少ないが、終了後に話しかけられるなどの行動はみられた。東北地域の方々とは、一度のセミナーだけでなく密に信頼関係を深めていく必要性を感じた。

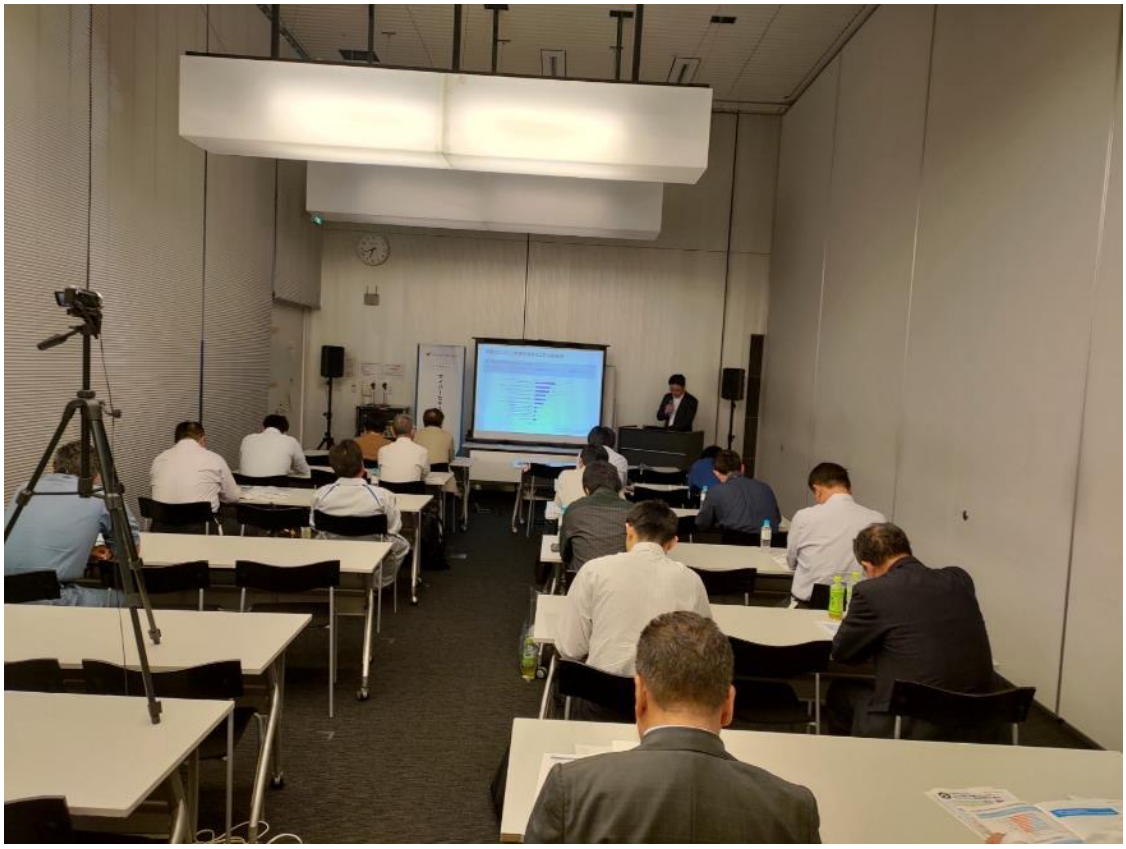


図 13.事業説明会風景（盛岡）

- 10/16 いわき（中止）

損保ジャパンが主催し 60 名の集客を見込んでいたが、10/12 に発生した台風 19 号の同地域での被災状況を受けて開催を中止した。

3-1-2. 事業説明会でのアンケートの結果

セミナー参加者向けに行ったアンケート（図 14）によると、業種は、サービス業、情報通信業、製造業が上位となっており、当初想定していた業種である一方で、宿泊業、医療・福祉といった個人情報を多く扱っていると思われる業種の参加が見受けられなかった。（n=57,9/5IPA セミナーでのアンケートを含む）

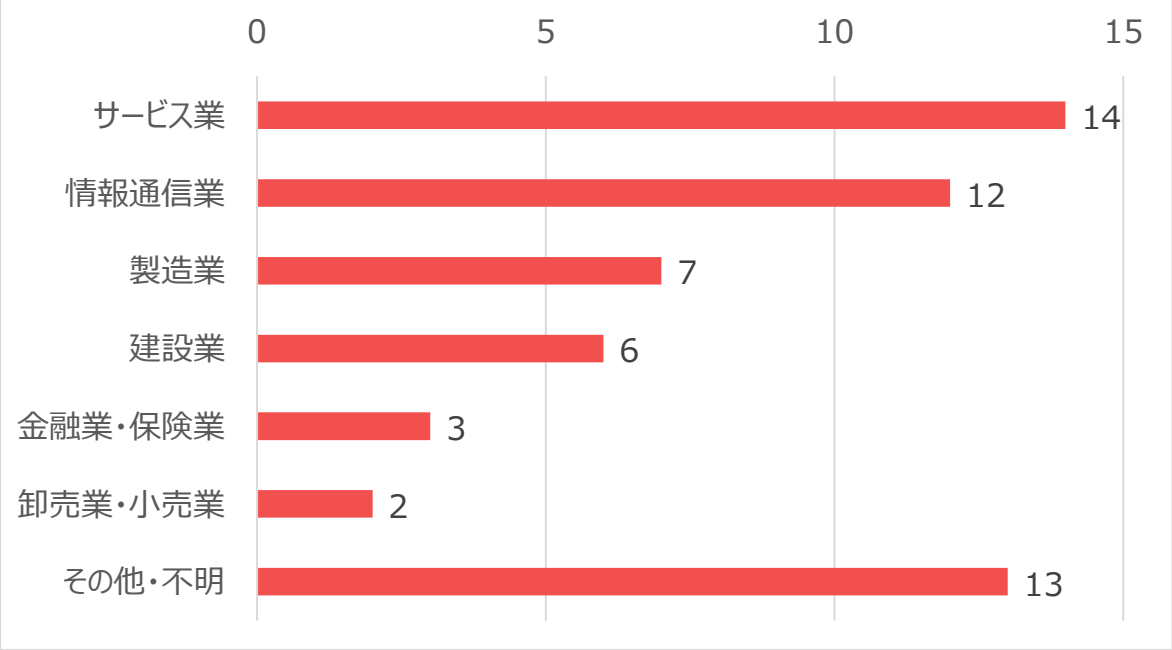


図 14.セミナー参加者アンケート結果（業種）（n=57）

また、セキュリティ対策の導入に関するアンケート（図 15）では、「ウィルス対策ソフト」「UTM/NGFW」「WAF」を導入済み・導入予定としている企業が多く、導入済み・予定のセキュリティ対策に対して、今後導入したいセキュリティ対策が多いカテゴリは、「セキュリティ監視サービス」「CSIRT」「EDR」「SoC」「SIEM」となり、監視系のニーズが高いことがうかがえる。ただし当事業自体が監視サービスを主体とするものであり、元々監視サービスに興味のある企業群が集まっていることは考慮すべき点である。

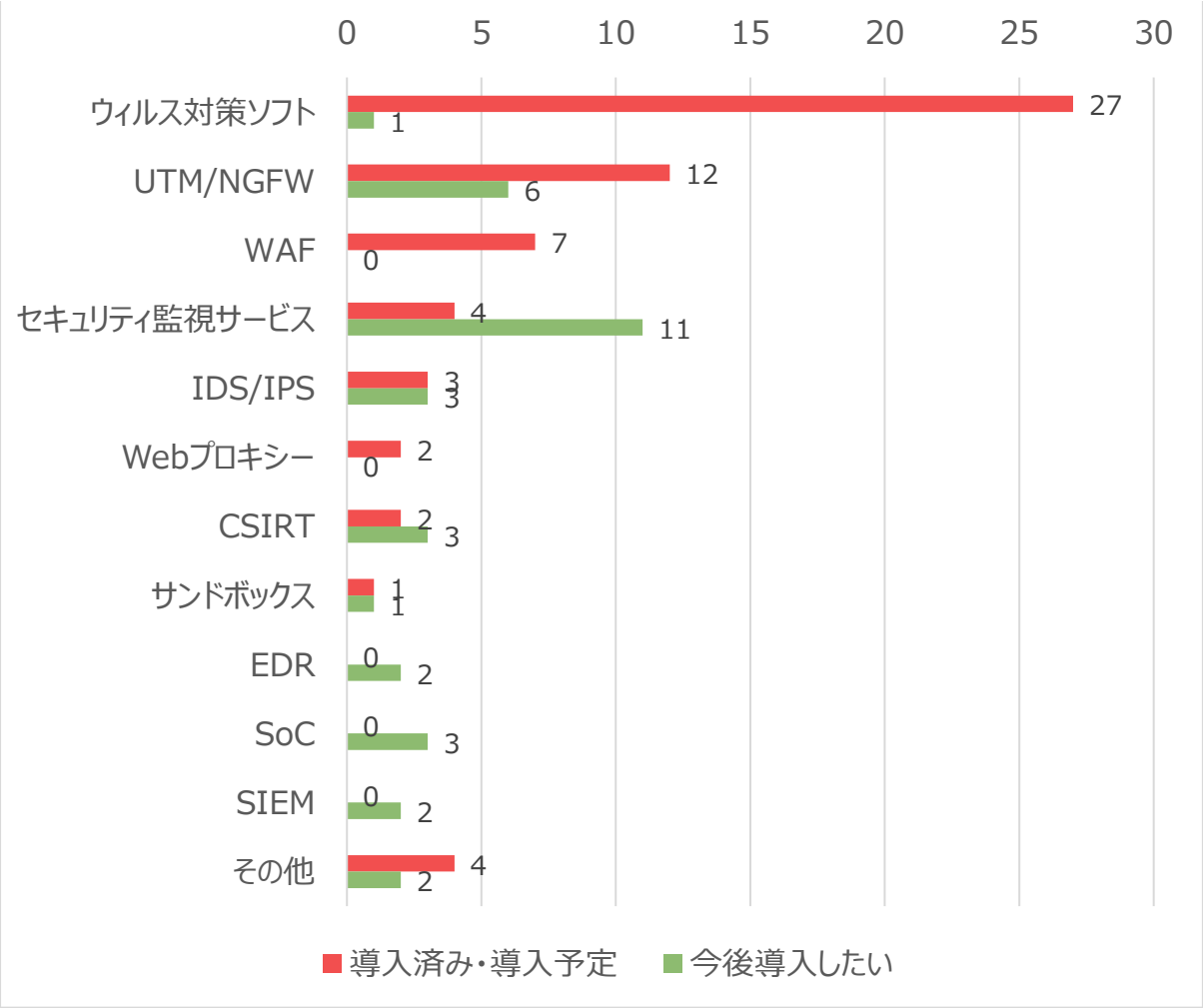


図 15.セキュリティ対策の導入に関するアンケート結果（n=57、複数回答あり）

3-1-3. 中間報告会

以下のとおり、中間報告会を実施した。

- 2019/12/11(水)15:00-17:00 仙台

場所：仙都会館
参加者数：26 名（25 社）
報告会の内容：
「事業実証中間報告」デジタルハーツ
「攻撃デモを見て学ぶユーザーフレンドリーなパスワード」株式会社セキュリティイニシアティブ
「中小企業における情報セキュリティ対策支援のご紹介」独立行政法人情報処理推進機構（以下「IPA」という。）

備考：
実証事業の中間報告のほか、地元でセキュリティの啓蒙活動を行っている地元企業の代表から、実際の攻撃デモの実演をしてもらうことで、脅威を身近に感じてもらう工夫を行い、参加者は真剣に話に聞き入っていた。質疑では IPA セキュリティプレゼンター[1]に関心が集まり、こうした公的機関と連携したセキュリティのセミナーを地元で行っていきたいという機運を感じた。

図 16.中間報告会風景（仙台）

[1]https://www.ipa.go.jp/security/keihatsu/sme/presenter.html

3-1-4. 成果報告会

実証参加企業や関係者に実証事業の最終的な成果を報告するために、以下の成果報告会を実施した。

- 2020/2/6（水）15:30-17:30 仙台

  場所：TKP 仙台東口ビジネスセンター　カンファレンスルーム
  参加者数：23 名（22 社）
  報告会の内容：
  「中小企業における情報セキュリティ対策支援のご紹介」IPA
  「最終成果報告・今後のあるべき姿について」デジタルハーツ
  「中小企業向けサイバー保険について」損保ジャパン

図 17.成果報告会風景（仙台）

３-２. 監視サービス

Starlight 上では多数のアラートが発生しており、これらについて SOC の監視員が分析・優先度付け（トリアージ）を行った結果、具体的対応が必要なセキュリティイベントは確認されなかった。セキュリティ上の懸念があるとして実証参加企業への詳細問合せを行ったケースとしては、以下のようなものがあった。

（１）2019/10/2 発生　卸売業
事象：POS レジから FTP への大量アクセス
措置：通信内容を事業者に確認したところ、POS 端末内のアプリ挙動と思われるものであるという回答があった。
結果：翌日以降に先方問題がないことを確認し、またアラート発報が収束していたことを確認したため、対応クローズ。

（２）2019/11/27 発生　卸売業
事象：RDP 通信（リモートデスクトッププロトコル）の急増
措置：発生状況を連絡。電話にて対象となる端末を確認されることを推奨。ソース IP の大多数が FW（Fortigate）であるとのことであり、恐らく、VPN 等を利用していることの影響と思われる。また、サーバに対して複数台の PC から RDP を使ってやり取りをする業務があるとのことであり、その関係の可能性が高い状況。
結果：実証参加企業側で対応・調査を検討するとのことであり、対応クローズ。

（３）2019/12/4 発生　サービス業
事象：不審ドメインへのアクセスが急増
措置：実証参加企業に確認したところ、心当たりがない、とのこと。また、当該端末は MAC アドレスから Apple 機器だが、業務で MAC-PC なりを利用されているか確認し、利用していない、とのこと。恐らく社内の Wi-Fi を使った個人の iPhone などの端末と思われるが、詳細は不明。
結果：実証参加企業の社内では心当たりがないとして、以後経過観察するとして対応クローズ。

3-2-1. 中小企業向けチューニング

本実証の開始後、いくつかの企業においてネットワーク遅延などの事象が発生したため、原因を調査したところ、インターネット接続の帯域が狭い企業や、導入している UTM/FW/インターネットルータのスループットが低い場合などに、インターネット遅延が発生していることが分かった。

このため、ネットワークセンサーから Starlight サーバに送付するデータのうち、Starlight の IDS 機能や Sandbox 機能については、キルチェーン後段である遠隔操作（Command & Control）、自動実行（Exfiltration & Actions）において検出が可能なことから、セキュリティ確保における問題が生じないものと考え、すべての実証参加企業に対し機能をチューニングして提供することとした。

3-2-2. 企業別分析

実証参加企業別に月別のアラート発生件数を集計した（表 2）。アラート発生件数は端末台数や通信量と通信内容、及び UTM/FW といったセキュリティ機器の導入の有無にも依存するものと考えられるため、Starlight にて検知した社内の端末台数、及び実証参加企業から取得したアンケート結果（一部未回答）から UTM/FW の設置の有無についても記録した。そして、1 端末・1 月あたりのアラート発生件数を集計したところ、以下のような結果となった。(表 1)

UTM/FW	月平均	端末数	端末平均
あり	8.4	65.24	0.31
なし・不明	4.2	19.90	0.58

表 1.1 端末/月あたりのアラート発生件数集計

こちらをみると、ネットワークに接続された端末の台数が多い企業ほど UTM/FW の導入が進んでいることが分かる。また、UTM/FW を導入していない（不明を含む）企業では、UTM/FW を導入している企業と比べて、1 端末・1 月あたりのアラート発生件数が 1.8 倍以上となっている。

こちらから推測されることは、UTM/FW を導入することでマルウェアの侵入などを抑えることができており、それによりアラート件数が少ないものと思われる。また、UTM/FW を導入している企業は他の企業と比較してセキュリティ意識が高いことが考えられ、そのような企業においてはウィルス対策ソフトの導入や OS・アプリのアップデート、アクセス権限の詳細な設定、利用者（従業員）への啓蒙、といったセキュリティ対策が他の企業と比較して進んでおり、それにより無用なアラートが発生していないということも考えられる。

これらのことから、UTM/FW などを導入していない企業に対しては、セキュリティ意識の向上につながるような啓発活動や、最初のステップとして UTM の導入などを行っていくことが効果的であると考えられる。

企業名	開始日	アラート数									UTM/FW	端末数	端末平均
		7月	8月	9月	10月	11月	12月	1月	合計	月平均			
A1社	2019/7/17	5	30	24	26	15	14	28	142	20.3	○	190	0.11
A2社	2019/7/17	0	1	0	0	0	0	0	1	0.1	○	46	0.00
A3社	2019/7/23	6	2	13	15	5	5	22	68	9.7	?	16	0.61
B1社	2019/8/1		2	4	12	6	12	0	36	6.0	○	15	0.40
B2社	2019/8/1		4						4	4.0	?		
B3社	2019/8/1		3	4	16	6	12	7	48	8.0	X	13	0.62
B4社	2019/8/2		2	1	14	3	5	3	28	4.7	X	18	0.26
B5社	2019/8/7		74	77	71	27	15	13	277	46.2	?	143	0.32
B6社	2019/8/7		6	11	21	20	3	10	71	11.8	?	131	0.09
B7社	2019/8/8		4	2	1	0	1	6	14	2.3	X	16	0.15
B8社	2019/8/8		2						2	2.0	?		
B9社	2019/8/9		1	22	6	14	19	12	74	12.3	X	43	0.29
B10社	2019/8/22		91	80	66	52	91	56	436	72.7	○	328	0.22
B11社	2019/8/27		3	15					18	9.0	?		
B12社	2019/8/28		0	2	3	2	2	1	10	1.7	?	56	0.03
C1社	2019/9/4			13	5	2	0	3	23	4.6	X	43	0.11
C2社	2019/9/11			1	0	0	5	0	6	1.2	X	3	0.40
C3社	2019/9/12			4	2	0	2	5	13	2.6	○	105	0.03
C4社	2019/9/13			9	25	27	15	4	80	16.0	?	27	0.59
C5社	2019/9/19			1	3	4	2	3	13	2.6	?	56	0.05
C6社	2019/9/19			2	1	1	2	0	6	1.2	○	5	0.24
C7社	2019/9/19			0	0	1	3	6	10	2.0	?	1	2.00
C8社	2019/9/19			0	0	2	6	2	10	2.0	?	4	0.50
C9社	2019/9/20			0	0	0	0	12	12	2.4	?	81	0.03
D1社	2019/10/4				19	30	20	6	75	18.8	○	34	0.55
D2社	2019/10/16				5	17	10	10	42	10.5	○	65	0.16
D3社	2019/10/17				7	12	12	14	45	11.3	○	329	0.03
D4社	2019/10/18				4	3	7	9	23	5.8	○	2	2.88
D5社	2019/10/20				0	0	0	0	0	0.0	?	6	0.00
D6社	2019/10/20				0				0	0.0	?		
D7社	2019/10/21				0	10	5	6	21	5.3	X	51	0.10
D8社	2019/10/21				0	0	0	1	1	0.3	○	7	0.04
D9社	2019/10/24				0	6	2	2	10	2.5	?	1	2.50
D10社	2019/10/24				0	1	1	2	4	1.0	○	8	0.13
D11社	2019/10/28				1	1	0	3	5	1.3	○	8	0.16
D12社	2019/10/28				0	0	1	0	1	0.3	○	8	0.03
D13社	2019/10/29				0	0	0	1	1	0.3	?	1	0.25
D14社	2019/10/29				2	5	4	9	20	5.0	X	20	0.25
D15社	2019/10/30				0	0	0	0	0	0.0	?	2	0.00
D16社	2019/10/31				0	0	0	3	3	0.8	?	2	0.38
D17社	2019/10/31				0	0	0	0	0	0.0	?	4	0.00
D18社	2019/10/31				0	13	9	3	25	6.3	?	17	0.37
D19社	2019/10/31				0	5	0	2	7	1.8	○	0	

表 2.企業別のアラート発報数と UTM/FW 有無の関連調査表（前半）

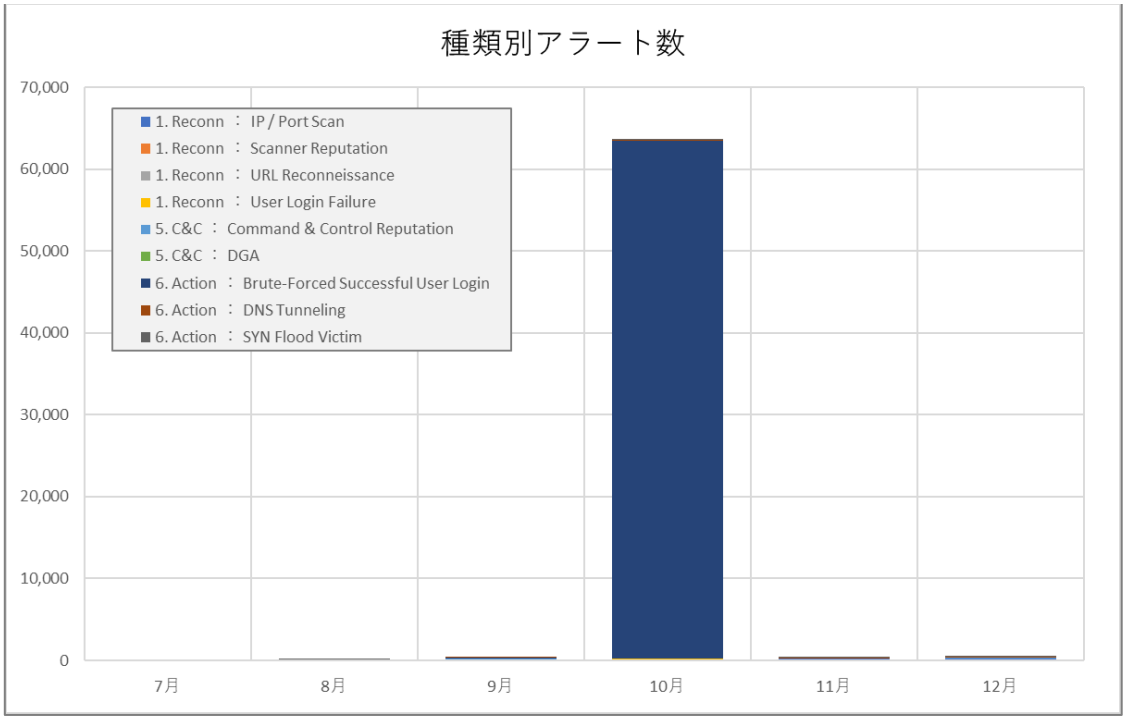
企業名	開始日	アラート数									UTM/FW	端末数	端末平均
		7月	8月	9月	10月	11月	12月	1月	合計	月平均			
E1社	2019/11/1					4	10	4	18	6.0	○	26	0.23
E2社	2019/11/1					1	2	8	11	3.7	○	89	0.04
E3社	2019/11/1					2			2	2.0	○		
E4社	2019/11/1					1	0	0	1	0.3	X	3	0.11
E5社	2019/11/2					0	1	0	1	0.3	X	3	0.11
E6社	2019/11/5					1	2	1	4	1.3	○	9	0.15
E7社	2019/11/6					8	6	14	28	9.3	?	84	0.11
E8社	2019/11/7					0	1	0	1	0.3	?	9	0.04
E9社	2019/11/7					0	0	1	1	0.3	?	6	0.06
E10社	2019/11/7					2	6	7	15	5.0	○	16	0.31
E11社	2019/11/8					2	0	1	3	1.0	?	1	1.00
E12社	2019/11/8					3	2	2	7	2.3	?	3	0.78
E13社	2019/11/8					0	0	0	0	0.0	X	2	0.00
E14社	2019/11/8					8	23	16	47	15.7	?	29	0.54
E15社	2019/11/8					1	6	2	9	3.0	?	3	1.00
E16社	2019/11/11					15	7	1	23	7.7	?	9	0.85
E17社	2019/11/11					0	0	0	0	0.0	?	1	0.00
E18社	2019/11/11					0	1	0	1	0.3	?	3	0.11
E19社	2019/11/13					4	0	0	4	1.3	X	1	1.33
E20社	2019/11/14					1	2	2	5	1.7	?	10	0.17
E21社	2019/11/14					0	0	0	0	0.0	?	1	0.00
E22社	2019/11/15					0	3	0	3	1.0	X	16	0.06
E23社	2019/11/15					1	1	1	3	1.0	?	0	
E24社	2019/11/15					0	2	0	2	0.7	?	2	0.33
E25社	2019/11/16					0	0	0	0	0.0	?	1	0.00
E26社	2019/11/18					0	0	1	1	0.3	?	0	
E27社	2019/11/19					0	0	0	0	0.0	?	3	0.00
E28社	2019/11/19					0	4	2	6	2.0	?	1	2.00
E29社	2019/11/19					1	4	5	10	3.3	?	6	0.56
E30社	2019/11/20					0	4	15	19	6.3	?	1	6.33
E31社	2019/11/20					0	0	0	0	0.0	?	1	0.00
E32社	2019/11/21					2	27	33	62	20.7	?	104	0.20
E33社	2019/11/22					1	8	16	25	8.3	○	21	0.40
E34社	2019/11/23					0	0	0	0	0.0	?	5	0.00
E35社	2019/11/25					1	16	25	42	14.0	X	112	0.13
E36社	2019/11/25					0	0	0	0	0.0	?	1	0.00
E37社	2019/11/25					0	0	0	0	0.0	?	0	
E38社	2019/11/26					0	0	2	2	0.7	X	12	0.06
E39社	2019/11/28					0	0	0	0	0.0	X	7	0.00
F1社	2019/12/3						2	7	9	4.5	?	9	0.50
F2社	2019/12/6						0	0	0	0.0	?	4	0.00
F3社	2019/12/9						0	12	12	6.0	?	5	1.20
F4社	2019/12/10						3	9	12	6.0	?	1	6.00
F5社	2019/12/20						1	6	7	3.5	○	59	0.06
合計		11	225	285	325	349	429	457	2,081	5.2			0.51

表 2.企業別のアラート発報数と UTM/FW 有無の関連調査表（後半）

3-2-3. 攻撃種類別分析

Starlight では CyberKillChain の各段階において、さらに様々な攻撃手法にセキュリティイベントを分類している。そして、各セキュリティイベントに対して AI が分析して危険性を示すスコア（0～100 点）をつける。そのスコアに応じて危険度を Critical（≧75 点）、Major（≧50 点）、Minor（≧25 点）、Notice（＜25 点）の 4 段階に分類してアラートを出すこととしている。

このうち、本実証のデータのうち Major 以上のアラートについて、攻撃手法ごとの集計を以下にしめす。(図 18)

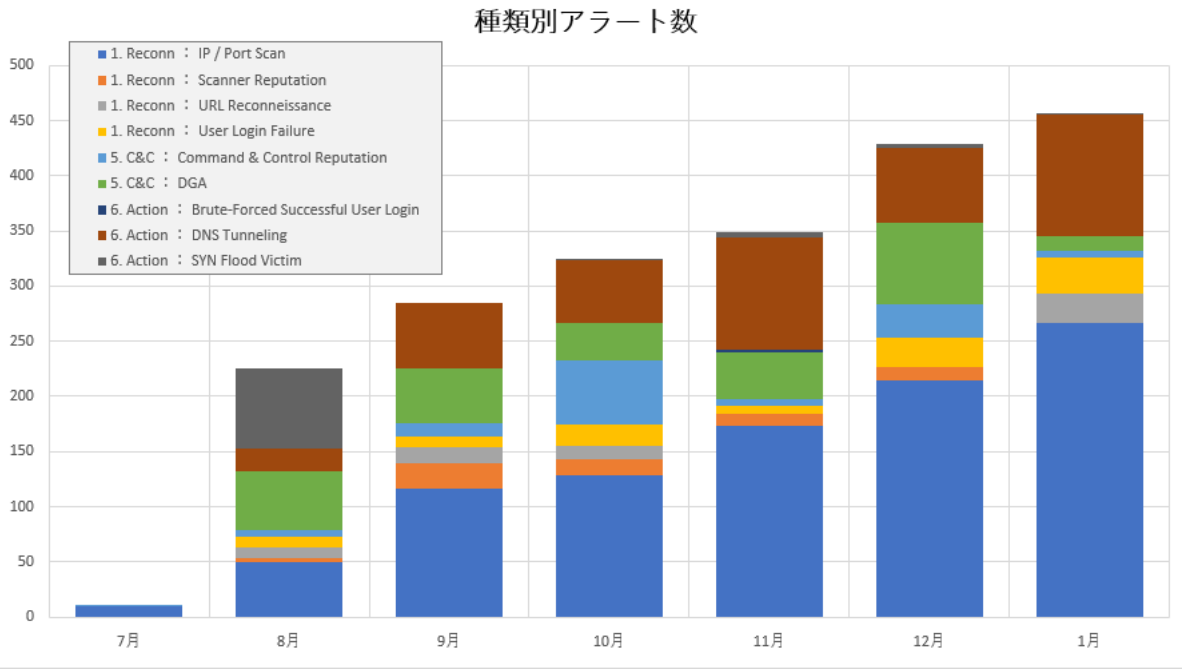


		7月	8月	9月	10月	11月	12月	合計
実証参加企業数		3社	15社	22社	40社	79社	82社	-
1. Reconn	IP / Port Scan	10	50	117	129	173	215	694
	Scanner Reputation	0	3	22	14	11	12	62
	URL Reconneissance	0	10	15	12	0	0	37
	User Login Failure	0	10	10	20	7	26	73
5. C&C	Command & Control Reputation	1	6	12	58	6	30	113
	DGA	0	53	49	34	43	74	253
6. Action	Brute-Forced Successful User Login	0	0	94	63,234	2	0	63,330
	DNS Tunneling	0	21	60	57	102	68	308
	SYN Flood Victim	0	72	0	1	5	4	82
	合計	11	225	379	63,559	349	429	64,952

図 18.攻撃種類別アラート数

10 月のアラート件数が突出しているが、こちらはある実証参加企業において POS レジの不具合により FTP サーバにおびただしいアクセスが発生したことによるものであり、問題がないことを企業の担当者に確認している（2019 年 12 月 31 時点）。

そこで、上記の不具合の誤検知を排除し、1 月分集計を追加した攻撃手法ごとの集計が下記のとおりである。(図 19)



攻撃フェーズ	イベント種類	7月	8月	9月	10月	11月	12月	1月	総計
実証参加機器設置企業数		3社	15社	22社	40社	79社	82社	81社	-
1. Reconn	IP / Port Scan	10	50	117	129	173	215	266	**960**
	Scanner Reputation		3	22	14	11	12	1	**63**
	URL Reconneissance		10	15	12			26	**63**
	User Login Failure		10	10	20	7	26	33	**106**
5. C&C	Command & Control Reputation	1	6	12	58	6	30	6	**119**
	DGA		53	49	34	43	74	13	**266**
6. Action	Brute-Forced Successful User Login					2			**2**
	DNS Tunneling		21	60	57	102	68	111	**419**
	SYN Flood Victim		72		1	5	4	1	**83**
合計		**11**	**225**	**285**	**325**	**349**	**429**	**457**	**2081**

図 19.攻撃種類別アラート数（誤検知排除後）

こちらをみると、Reconn フェーズの IP/Port Scan や Action フェーズの DNS Tunneling の件数が多数検出された。これらのアラートについての詳細分析を行った。

3-2-4. *IP・Port Scan* 分析結果

アラートが最も多数発生していた IP・Port Scan のアラート内容について詳細分析を行った。このアラートでは、サーバの特定のポートまたはポート範囲に対して通常より高い頻度で通信・切断を行っている場合を検出する。

まず、通信元と通信先が社内のプライベートアドレスか社外のパブリックアドレスかを分類した(表3)。

送信元	送信先	7月	8月	9月	10月	11月	12月	1月	合計
private	private	1	2	9	10	14	24	11	71
	public	9	39	89	107	157	185	254	840
public	private			1					1
	public		9	18	12	2	6	1	48
合計		10	50	117	129	173	215	266	960

表 3.月別 IP・Port Scan アラート件数

パブリックからの IP/Port Scan は特定の 1 企業においてのみ発生していたが、こちらの社内でパブリック IP アドレスを利用しているために発生しており、社外からの攻撃ではなかった。

また、6 件のアラートを除くすべてのアラートについて通信元及び通信先の信頼情報（Reputation）は Good であり問題はなかった。

6 件のアラートは通信先の信頼情報が Good 以外であったが、通信先について調査したところリモートアクセスサービスで提供されている中継サーバであり、これら 6 件についても問題はなかった。

以上のことから、これらのアラートについてインシデント対応は不要なものと判断した。

3-2-5. *DNS Tunneling* 分析結果

次に、2 番目にアラート発生数の多かった Action フェーズの DNS Tunneling について詳細調査を行った(表 4,表 5)。DNS Tunneling は、インターネットでよく利用される DNS のリクエスト・レスポンスを利用して、DNS のフリをした C&C サーバと通信を行う手法であり、マルウェアや侵入者が C&C サーバからの命令を受けたり、C&C サーバから情報を漏洩させたりする場合などに利用される。このアラートでは、クエリ内容が複雑な DNS クエリを検出している。

ドメイン	判定	件数
cedexis-radar.net	?	8
e5.sk	?	22
online-metrix.net	?	20
webcfs06.com	?	1
44ihxbbbzq1u2qdphznphljce1.com	X	1
ax2vp12cubd7qnd6adj8otx1wv.com	X	1
bxhyolm0fgvttr87fkqf7honjga.com	X	1
bxjqkiyhp9yqogzy7rjv8p.com	X	1
cx8b2xpoyiqh.com	X	1
dm1jvigtf4bbvlks3gvhhsh4.com	X	1
ek7gyoyocct0gtmwrwtr66j9r.com	X	1
feqw1x5synj9fqww7.com	X	1
fsxsrwvd-i4ow4kw6keq.com	X	1
g6pfbozovknd17orld7bb7jb.com	X	1
gewrsjdp779mz4kkouz4.com	X	1
gg1s5hgijrxgh8-bkq1a2cmk2i1.com	X	1
gnotomjglc6gly40n2phcvbsl1a.com	X	1
hvx4k7xsw1eq1p.com	X	1
iqdo1dcfoaaaw17b1csxhu5qz.com	X	1
jmulkzgiwsxb2wdxlej8lqi0r0.com	X	1
khx1k1m7xveji8dniqhwv8iyy1.com	X	1
lngwhha4o3aj8uqufvd.com	X	1
mjmo1gbmwo6zvwkswhe.com	X	1
mossqzr1dpvmsk12kysyc3m143v.co	X	1
njhwlklbjmyu.com	X	1
nzwujv5v3lc0esdf.com	X	1
pbosdfr7kynrq8-nwtzmc1e.com	X	1
pckh6n48gl8s3pnetvxynnowc.com	X	1
pwxx13ku2nf8s89qakq7-e7jwm4.co	X	1
qrq4sq0wvgfyg7zl2fo33zpzbp.com	X	1
s3v6xcdryyaprpne.com	X	1
sp1e4uz6evbordvpju.com	X	1
tt87ci85lfut6o1zlh1m7x.com	X	1
u5bb9ezkjbxrowu74ejd.com	X	1
veqsdumh.com	X	1
vq6ef7i9fwprb0dh1t7fc9.com	X	1
vzgtjbyluojhcmu.com	X	1
wdplxeffx2h2y0mul7p139.com	X	1
wh0ilwfx5kdz7lkjki9wj5snx.com	X	1
wvmteelglzeqn1yo3fffttva09.com	X	1
xqfum4y8ev6f8oduhy5htgrq1.com	X	1
yl1ww3v6kqzx1txf.com	X	1
ysqlg5syun.com	X	1
zbhywwupn99h8stsg7vj.com	X	1
zgezdenbqheytqmrxtitanium00	X	1
zvvg92ettwxlkca80vy2uj3y0d.com	X	1

表 4.通信先ドメインの判定と通信件数

判定	件数	割合
○	326	78%
?	51	12%
X	42	10%
合計	419	100%

表 5.ドメイン名別判定結果の件数と割合

DNS のクエリ内容にあるドメイン名を調査したところ、78%は AWS や Azure、Google などのクラウドサービスへのアクセスであり問題はなかった。動的に生成された長いサーバ名であるため誤検知をしたと考えられる。

続いてアラートの 12%を占める 4 個のドメイン名は、ドメイン取得業者が不明であったが、調査したところセキュリティサービスやマーケティングサービスで利用されており、問題はないものと考えられる。

残りのアラートの 10%を占める 42 個のドメインは、マルウェアなどで DGA と組み合わせて一時的に利用されていたドメインである可能性が高いと思われるが、現在ドメインの登録がなくなっており、現時点における脅威はないと考えられる。

以上により、これらのアラートに関してもインシデント対応が必要な脅威はないものと判断した。

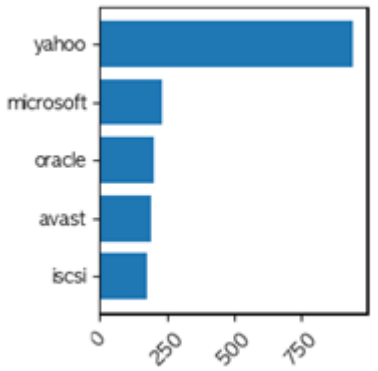
3-2-6. その他フェーズでの分析結果

前項でアラート件数上位である IP・Port Scan 及び DNS Tunneling の分析を行ったが、それ以外のフェーズでのアラート分析についても、脅威はないことを確認した。

3-2-7. アプリケーション（プロトコル）別の上位アクセス状況

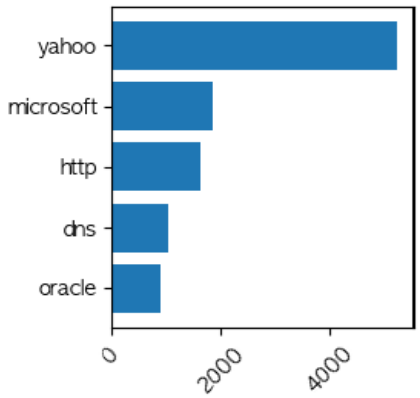
ネットワークセンサーで取得したログのうち、通信の多かったアプリケーションは以下のとおりとなる。
なお、2019 年 7 月度、及び 8 月度については、アラート数の取得となるが、9 月以降については利用状況把握のため、セッション数の取得とした。

実証参加企業増加に応じてセッション数が増加しており、また月ごとに利用構成が常に入れ替わっていることから、企業ごとに利用アプリケーションの利用が異なっていることが分かった。



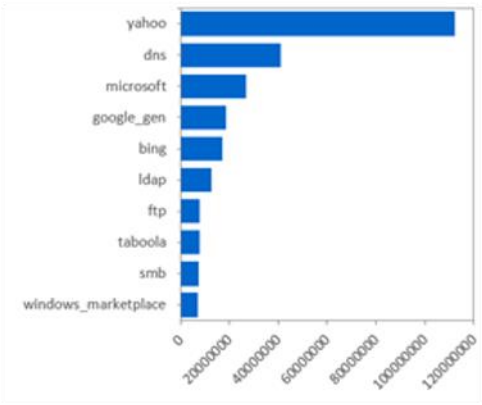
アプリケーション	アラート数
yahoo	941
microsoft	233
oracle	203
avast	192
iscsi	178

図 20.2019 年 7 月度アプリケーション別アラート数



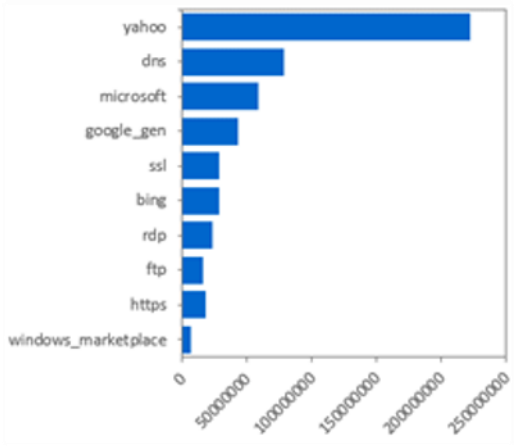
アプリケーション	アラート数
yahoo	5231
microsoft	1866
http	1625
dns	1039
oracle	884

図 21.2019 年 8 月度アプリケーション別アラート数



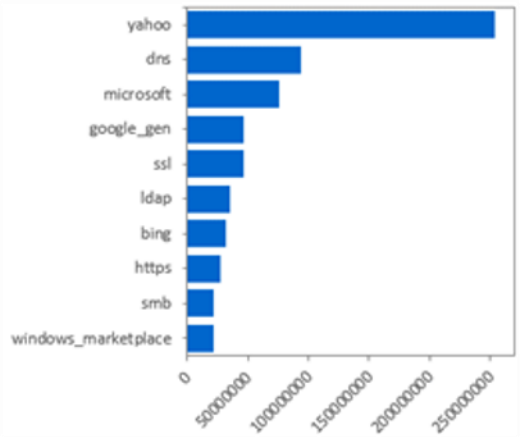
アプリケーション	セッション数
yahoo	112313521
dns	41149571
microsoft	27000749
google_gen	18706263
bing	17286374
ldap	12501506
ftp	7731110
taboola	7617149
smb	7253370
windows_marketplace	6896471

図 22.2019 年 9 月度アプリケーション別セッション数

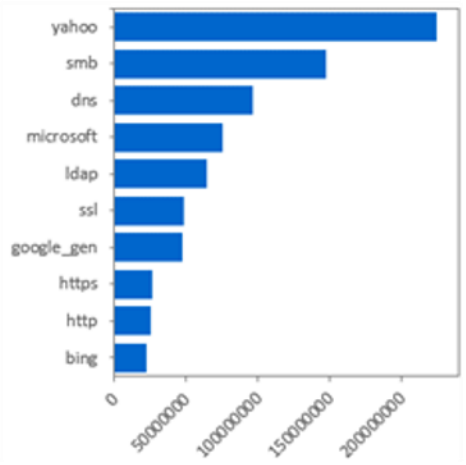


アプリケーション	セッション数
yahoo	222902982
dns	78912819
microsoft	58710841
google_gen	42851281
ssl	28708202
bing	28576896
rdp	23337598
ftp	15577407
https	17633614
windows_marketplace	6896471

図 24.2019 年 11 月度アプリケーション別セッション数

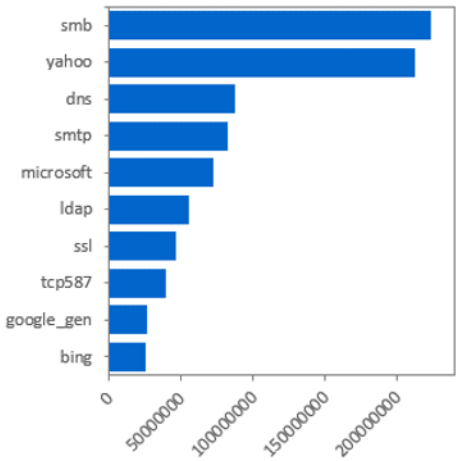


アプリケーション	セッション数
yahoo	253675574
dns	93836088
microsoft	75739258
google_gen	46723057
ssl	46112928
ldap	35243172
bing	31990467
https	27604162
smb	21922666
windows_marketplace	21240549



アプリケーション	セッション数
yahoo	224049539
smb	147321517
dns	96879236
microsoft	75160848
ldap	64178782
ssl	47974377
google_gen	47393094
https	26789502
http	25711228
bing	22414853

図 25.2019 年 12 月度アプリケーション別セッション数



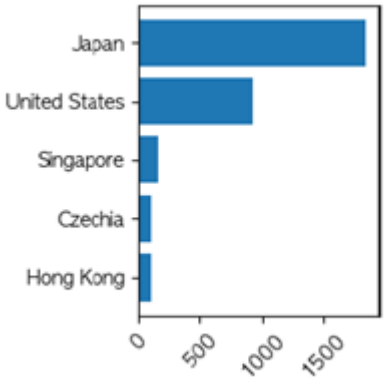
アプリケーション	セッション数
smb	223085932
yahoo	212571637
dns	87436782
smtp	82024646
microsoft	72549256
ldap	55261748
ssl	46205511
tcp587	39050246
google_gen	26387376
bing	25356705

図 26.2020 年 1 月度アプリケーション別セッション数

3-2-8. 通信先（国家）別の上位アクセス状況

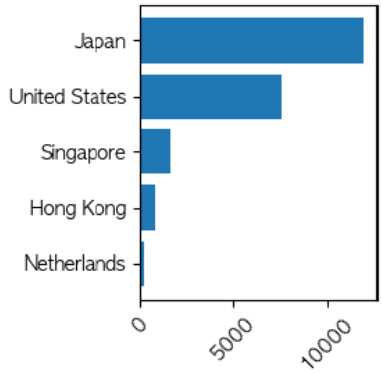
ネットワークセンサーで取得したログのうち、通信の多かった通信先は以下のとおりとなる。
なお、2019 年 7 月度、及び 8 月度については、アラート数の取得となるが、9 月以降については利用状況把握のため、セッション数の取得とした。

実証参加企業の増加に応じてセッション数は月ごとに増加しているものの、通信先の構成については大きな変化がないことが分かった。



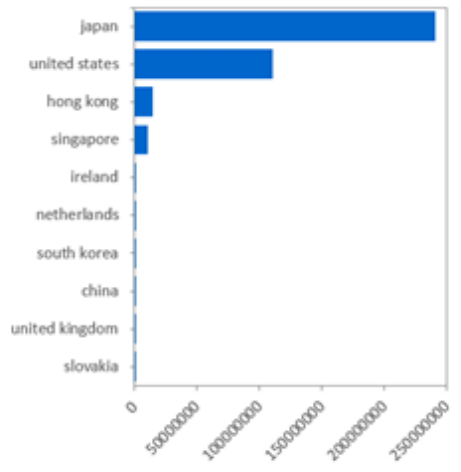
通信先国家	アラート数
Japan	1841
United States	923
Singapore	157
Czechia	106
Hong Kong	100

図 27.2019 年 7 月度通信先別アラート数



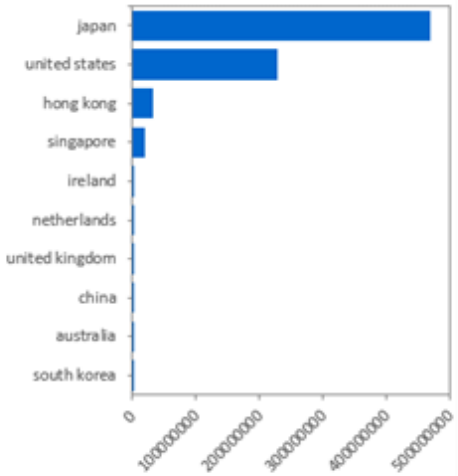
通信先国家	アラート数
Japan	11940
United States	7541
Singapore	1623
Hong Kong	833
Netherlands	216

図 28.2019 年 8 月度通信先別アラート数



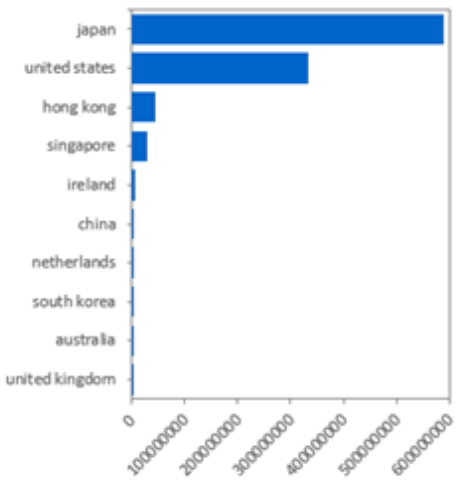
通信先国家	セッション数
japan	241026865
united states	110820153
hong kong	15051555
singapore	10734134
ireland	1505172
netherlands	890989
south korea	584217
china	472935
united kingdom	407792
slovakia	381882

図 29.2019 年 9 月度通信先別セッション数



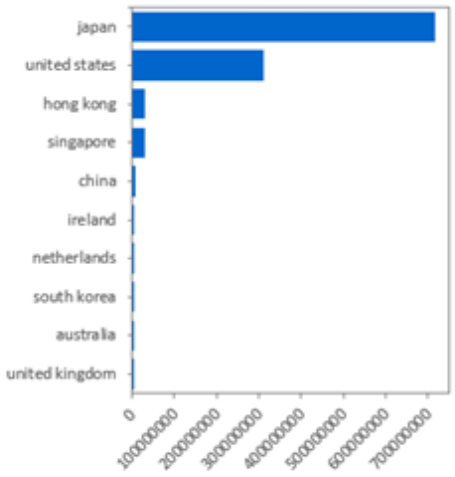
通信先国家	セッション数
japan	470425916
united states	229675092
hong kong	32516523
singapore	20773752
ireland	3141487
netherlands	2158047
united kingdom	1210937
china	1197907
australia	1019065
south korea	1002721

図 30.2019 年 10 月度通信先別セッション数



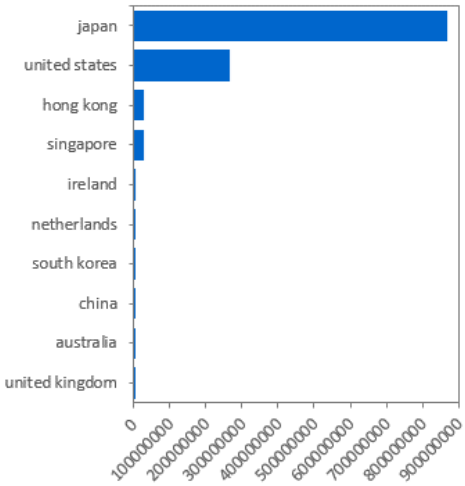
通信先国家	セッション数
japan	589620379
united states	333096840
hong kong	43341256
singapore	28158175
ireland	5090528
china	3504173
netherlands	3464746
south korea	3124980
australia	2620109
united kingdom	1627412

図 31.2019 年 11 月度通信先別セッション数



通信先国家	セッション数
japan	717530211
united states	310691603
hong kong	30474599
singapore	29055375
china	7973974
ireland	5106471
netherlands	3940225
south korea	3339947
australia	2455366
united kingdom	1878017

図 32.2019 年 12 月度通信先別セッション数



通信先国家	セッション数
japan	866907282
united states	267352448
hong kong	29353497
singapore	27645497
ireland	4846696
netherlands	3483403
south korea	2779839
china	2556392
australia	2249480
united kingdom	1385209

図 33.2020 年 1 月度通信先別セッション数

3-3. 事後対応支援

3-3-1. インシデント対応

本実証では、インシデント対応による駆けつけサービスを 2 件実施した。

なお、インシデントは、デジタルハーツにて不正通信を検知や、実証参加企業にてサイバー攻撃を受けたと思われる事象が発生し、それを調査・確認をした上で、セキュリティリスクがあると判断されたものについてインシデントとした。

（1）インシデント対応 1

1. 対応概要
   Emotet 感染による被害拡大防止対策の実施、駆除対応の実施、事後対応案の提示

2. 対象企業
   岩手県の食品製造業 A 社（以下、A 社）
   資本金：1000 万円
   従業員数：6-20 名

3. 実証参加経緯
   [10/6]ウェブサイト経由で A 社から実証参加を希望する旨の問合せをいただく。「工場内の IT 活用を進めるにあたりセキュリティ面での向上も図っていきたい」という動機。

   [10/16]デジタルハーツの担当が A 社を訪問して事業内容を説明し、実証参加に同意。

   [10/30]デジタルハーツが設置のために訪問したが、ネットワーク構成上の確認が必要な点（一部の無線クライアントの監視を対象に含めるか否か）があったため、作業を中断。A 社と相談の上、実証段階では現状のネットワーク構成のまま一部の機器の監視を行うこととして、デジタルハーツの担当が再訪問することとした。（A 社は本実証の結果を踏まえて UTM の導入を検討したいとのこと）

   [11/8]監視センサーを設置。同日より監視を開始した。

4. SECURITY ACTION 参加状況
   二つ星

5. インシデント対応履歴

[11/19]
10:05 デジタルハーツのドメインメール宛てに A 社を装ったメールを受信①

13:00 A 社へ電話にて速報連絡。
―外部関連機関からの申告により A 社は 11/15 時点で認識していた。
―11/15 にメールパスワード変更等を実施済み
―11/15 に PC 全台フルスキャンしておりマルウェアは発見できなかった
―外部金融機関より「Emotet 感染の疑いがある」と指摘があった
―A 社にて当該端末を隔離し、当該端末以外の PC 初期化を実施した。
※この段階でメールサーバ、またはメールクライアント内のデータが抜き出されたと推定

[11/20]
15:00 デジタルハーツの技術者が A 社を訪問し、オンサイトにてインシデント対応開始
―当該端末にてマルウェアのプロセス起動・存在状態の確認を実施
―メールサーバ（レンタルサーバ）のログ取得を実施
21:30 オンサイトでのインシデント対応完了
※ログ内容、メール運用状況確認したところ、メールサーバからデータが抜き取られた可能性は低く、クライアント PC 側の対策を行う方向で検討

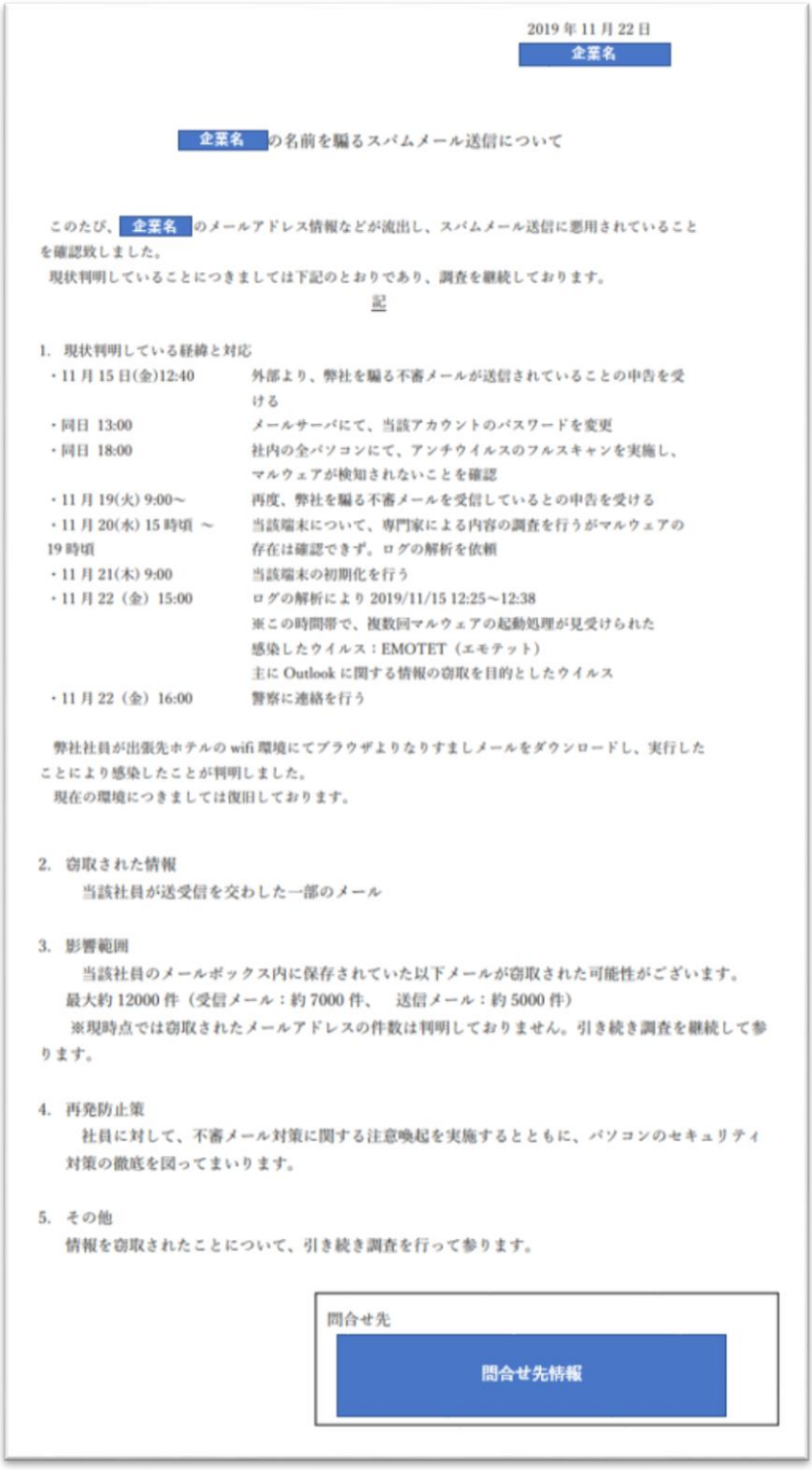
[11/21]
08:49 デジタルハーツのドメインメール宛てに A 社を装ったメールを受信②
A 社にて当該端末の初期化の実施
午後デジタルハーツにてインシデント分析を実施
―Emotet 感染により悪性 PowerShell コマンドが実行されていることを確認
―抜き取られたアドレス情報からスパムメール送信に悪用されていると推測
―外部メールサーバを利用して、抜き取ったメールに対して返信する方式で スパム配信していると推測

[11/22]
11:34 A 社へ分析結果、及び対応方法をメールにて提示
―PowerShell を禁止設定にする対策の提示
―不正通信先ホスト及び IP のアクセスブロックを提示
―アンチウィルス、OS、ブラウザの最新版バージョンアップを推奨
―経緯についてホームページで告知する場合の案を提示

14:26 A 社より今後の対応方法について連絡あり
―警察への連絡

―経緯についてホームページで告知（警察報告も含め）
―PowerShell の禁止設定、他の対策を実施する

16:00 A 社により警察に連絡を行った
A 社 Web サイトに案内を掲載(図 34)



2019 年 11 月 22 日
企業名

企業名の名前を騙るスパムメール送信について

このたび、企業名のメールアドレス情報などが流出し、スパムメール送信に悪用されていることを確認致しました。
現状判明していることにつきましては下記のとおりであり、調査を継続しております。

記

1. 現状判明している経緯と対応

・11 月 15 日(金)12:40	外部より、弊社を騙る不審メールが送信されていることの申告を受ける
・同日 13:00	メールサーバにて、当該アカウントのパスワードを変更
・同日 18:00	社内の全パソコンにて、アンチウイルスのフルスキャンを実施し、マルウェアが検知されないことを確認
・11 月 19(火) 9:00～	再度、弊社を騙る不審メールを受信しているとの申告を受ける
・11 月 20(水) 15 時頃 ～ 19 時頃	当該端末について、専門家による内容の調査を行うがマルウェアの存在は確認できず。ログの解析を依頼
・11 月 21(木) 9:00	当該端末の初期化を行う
・11 月 22（金）15:00	ログの解析により 2019/11/15 12:25～12:38 ※この時間帯で、複数回マルウェアの起動処理が見受けられた 感染したウイルス：EMOTET（エモテット） 主に Outlook に関する情報の窃取を目的としたウイルス
・11 月 22（金）16:00	警察に連絡を行う

弊社社員が出張先ホテルの wifi 環境にてブラウザよりなりすましメールをダウンロードし、実行したことにより感染したことが判明しました。
現在の環境につきましては復旧しております。

2. 窃取された情報
当該社員が送受信を交わした一部のメール

3. 影響範囲
当該社員のメールボックス内に保存されていた以下メールが窃取された可能性がございます。
最大約 12000 件（受信メール：約 7000 件、 送信メール：約 5000 件）
※現時点では窃取されたメールアドレスの件数は判明しておりません。引き続き調査を継続して参ります。

4. 再発防止策
社員に対して、不審メール対策に関する注意喚起を実施するとともに、パソコンのセキュリティ対策の徹底を図ってまいります。

5. その他
情報を窃取されたことについて、引き続き調査を行って参ります。

問合せ先
問合せ先情報

図 34.A 社が掲載した WEB ページ

6. 補足
当インシデントは、デジタルハーツが設置した監視センサーで検知されたものではなく、デジタルハーツ宛てに送付された偽装メールをきっかけとした対応。

（２）インシデント対応２

1. 対応概要
   悪質サイトへ誘導すると思われる広告のブロック対応

2. 対象企業
   宮城県の士業 B 社（以下 B 社）資本金：1000 万円未満
   従業員数：6～20 名

3. 実証参加経緯
   [9/11]仙台開催の事業説明会に参加いただく。現在運用している外部ベンダーが信用できないとのことで、セキュリティ対策についての相談を含め信頼できるパートナーを探しているとのこと。

   [10/18]デジタルハーツの担当者が訪問して詳細説明後、設置予定であったが、ネットワーク構成上の確認が必要となり、設置を延期。

   [11/7] 監視センサーを設置。同日より開始した。

4. SECURITY ACTION 参加状況
   取得なし

5. インシデント対応履歴
   ----------発生時の B 社での対応----------

   [12/12]
   12:55
   B 社のスタッフにて rednews7.com にアクセス（Chrome のブラウザ利用）サイトを開いたときに怪しい画面が表示された。日本語が変だったのですぐに画面を閉じた。

   15:03
   Windows のデスクトップ画面の右下（タスクバーあたり）に偽の通知が表示されるようになった。うっかりクリックしたら、Chrome が起動し、サイトが表示されたのですぐ閉じた。（canselism[.]com）メモが取れなかったが、php クエリストリームが続いていた。

15:10

当該端末の LAN ケーブルを抜いた。その後、LAN ケーブルを抜いた状態で、また偽の通知が表示されたためクリックすると、別サイトに誘導された。
（NW につながってないのでアクセスはしてない）
（mediabasket[.]club）

----------以下からデジタルハーツにて対応----------

15:30

デジタルハーツの問合せ窓口に入電。B 社内の PC がマルウェア感染したおそれがあるとのこと。デジタルハーツにて状況を確認し、対応策を検討の上、駆けつけ訪問を実施することをお伝えした。

[12/17]

17:00

駆けつけ対応にて先方へ訪問し、以下の対策を実施した。

(1)当該端末の状況確認
実際にネットワーク接続し Chrome(通常利用しているブラウザ)を立ち上げたところ、広告が PC 右下に表示される

(2)下記 URL を参考に当該ドメイン<rednews7[.]com>のブロックを実施した
https://[redacted]

(3)端末の再起動後再度広告が出るかを確認した
Chrome にブロックの登録を実施したため再起動し広告が表示されるかを確認したところ表示されなくなったことを確認した

(4)不審なプログラム確認
当該端末に不審なプログラムが意図せずインストールされていないかを確認した
コントロールパネルのプログラムの機能で確認したインストールされたプログラムのキャプチャを取得し、すべて確認したところ特に不審なプログラムは確認できなかった

(5)不審な拡張機能の確認
Chrome に不審な拡張機能が追加されていないかを確認した
拡張機能のキャプチャを取得いただきすべて確認したところ特に不審な拡張機能は確認できなかった

(6)Chrome のホームボタン及び起動時のページを確認した
ホームボタンに不審なウェブアドレスは特に登録されていないことを確認した
起動時特定のページが開かれる設定になっていないことを確認

(7)Chrome のクリーンアップ
Chrome の機能である「有害なソフトウェアの検出」を実施
有害なソフトウェアが検出されなかったことを確認

(8)Chrome の設定リセット
設定のリセットを実施。リセットされるのは以下
・起動ページ
・新しいタブページ
・検索エンジン
・固定タブのリセット
・拡張機能の無効、cookie の一時データ削除

(9)ブロック設定
Chrome の設定をリセットしたことで （２） で実施したブロックもリセットされたため 、再度<rednews7[.]com>のブロックを実施。
※（８）の時点で広告はでないことを確認いただいているが （９） の項目は念のための実施

(10)実証参加企業へ報告
実証参加企業に報告し実証参加企業に当該端末を操作いただき広告が表示されていないことを確認。
当被害において、Stellar Cyber のログの確認を行ったが、被害の兆候などを検知するログは見当たらなかった。
考えられる理由としては、当該サイトが https 通信であり、かつマルウェア配布サイトや C&C サイトでなく、セキュリティベンダー側で「clean」とされたアドウェアサイトであったため、Stellar Cyber では検知できなかったと思われる。

6. 考察
悪質サイトへ誘導する広告表示の通知を誤って許可してしまったことにより、意図しないポップアップ広告が表示されてしまった事案と思われる。
ユーザー側で任意で広告表示を許可してしまっているため、不審メール受信時の対応と同様に、「ユーザーにとって知らないポップアップが出た場合は許可せずブロックし、不明であれば管理者に確認する」といった対応が必要となり、対策としては社内

でのリテラシーの向上のための研修や不正メール・不正通知に対するトレーニングなどとなるかと思われる。

3-3-2. 問合せ

- 相談受付総数（電話での問合せも含む）：16 件

通信速度遅延に関する問い合せ　　6 件
センサー機器を設置後に社内のネットワーク通信速度やインターネットの表示速度の低下がみられたため、原因調査のためのヒアリングと解決方法の案内
速度改善がみられない場合は、センサー機器の撤去手配の案内

サービスに関する質問　4 件
センサー機器の仕様に関する質問、分析システムに関する質問、レポート内容や発行タイミングに関する質問など

監視機器の一時停止時の相談　　3 件
事務所移転、ビル内定期停電、ルータや UTM の新規導入・入れ替えに伴うネットワーク構成変更によりセンサー機器の一時撤去または電源 OFF が必要となる場合の対処方法の案内

インシデントに関する対応　　2 件
「事後対応支援」に関する問合せ対応

セキュリティ対策に関する相談　1 件
現状導入しているウィルス対策ソフトの評価に関する相談

３-４. 情報ポータル

３-４-１. 実施内容

本実証事業の紹介、問い合せ窓口、サイバーセキュリティに関する情報提供等を行うポータルサイトを開設した(図 35,図 36)。

開設日　：2019 年 8 月 22 日

情報ポータルは、本実証事業の内容を機器設置企業のみに閉じたものとすることなく、広く地域の意識啓蒙を目的として設置した。サービス内容や説明会の案内・開催資料の掲載をするほか、IPA 等が発信する情報を掲載することにより、東北地域の中小企業がサイバーセキュリティに関して情報収集する際の起点となるものとすることを心がけた。また、本活動を実証期間中に限定することなく、今後も継続して情報発信等を行っていくためのプラットフォームとして位置づけることを目的とした。

ただし、東北地域の中小企業はインターネットからの情報収集はあまり積極的に行っていない実情を踏まえれば、サイバーセキュリティに関するセミナーや、東北地域でのマルウェア感染事例など、具体的に関心がある情報をきっかけに、情報ポータルサイトでその詳細や対策を知ることができる、といったリアルコンテンツとの連動性が非常に重要となる。また、こうした取組みは短期的に効果が出るものではなく、継続して発信していくことによる累積効果が期待されるものであるため、実証事業の終了後も、自主的に運営して地元経済団体等の活動と連携していく方針とした。

図 35.ポータルサイトのイメージ（１）

図 36.ポータルサイトのイメージ（２）

- 実証ポータルで提供した情報について

イベント情報：事業説明会やセミナーなどの開催告知、及び開催内容の掲載　　6 件
セキュリティニュース：脆弱性情報、注意喚起、　　6 件
関連情報：台風被災関連、QA 掲載　　2 件
実証情報：実証結果など　　0 件

- アクセス状況（1 月 3 1 時点）

ユニークユーザー数：1,257
セッション数：1,772
ページビュー数：4,265

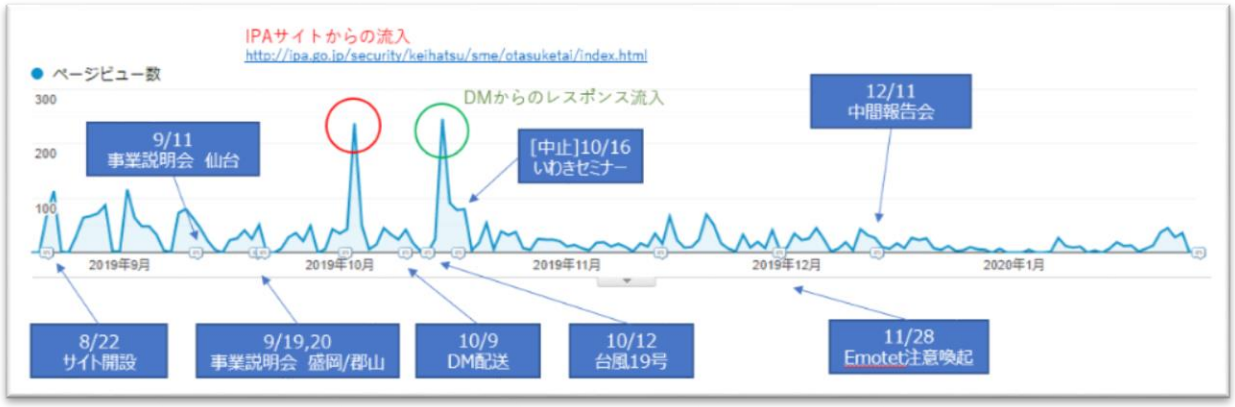


図 37.ポータルサイトのページビュー推移

アクセス状況を見る限り、WEB サイト単体での情報発信手段としては効果が薄い。実証情報など当サイトでしか得られない情報を定期的にアップデートしてコンテンツを充実させるとともに、セミナー、メルマガ、DM などリアルコンテンツとリンクすることにより、効果を高めることが見込める。

3-5. 実証参加企業

3-5-1. 実証参加企業の募集活動

- 自社及び地場企業での開拓

　デジタルハーツの仙台事業所での既存取引企業・関与企業に対して、直接アプローチを実施した。また、東北エリアに既存顧客を有する地場企業から、既存顧客へアプローチしていただく形で実証参加企業を開拓した。なお、地場 IT ベンダーには、機器設置や駆けつけ対応などの業務も併せて委託した。

・株式会社アライブ（企業開拓、機器設置業務委託、駆けつけ対応業務の委託）
・株式会社セント（企業紹介）
・テクノマインド株式会社（企業紹介）
・損保ジャパン（企業紹介）

- 地域団体からの紹介

　各地域団体の会員企業に対して、団体から紹介をいただき、同行にて訪問・説明を行う形で勧誘活動を行った。

・宮城県中小企業団体中央会（組合員の紹介）
・協同組合仙台卸商センター（組合員企業の紹介）
・仙台自動車整備工業団地協同組合（組合員企業の紹介）
・一般社団法人みやぎ工業会（会員企業の紹介）
・一般社団法人宮城県情報サービス産業協会（メーリングリストへの周知）
・公益財団法人仙台市産業振興事業団（メーリングリストへの周知）
・宮城県損害保険代理店業協会（古川支部）（会員向け説明の機会の提供）
・岩手県商工労働観光部ものづくり自動車産業振興室（いわて産業振興センターの紹介）
・いわて産業振興センター（メーリングリストへの周知）
・岩手県一関水道工事業協同組合（組合員企業の紹介）

- ダイレクトメール

直接募集を行う方法として、郵送によるダイレクトメール約 9,700 通の配送を実施した(図 38)。対象業種は、サプライチェーンの観点から、運送業、建設業、製造業、販売業を選定し、個人情報保護が重要と思われる業種として、IT サービス業、宿泊業、士業、証券・保険業、旅行業を併せて選定した。配送エリアは、商業が活発である宮城県仙台市、岩手県盛岡市、福島県郡山市を選定した。また、P マーク取得企業約 250 社に対して、追加で DM 配送を行った。なお、ダイレクトメール発出に際しては、経済産業省及び IPA の連名による添え状を添付することとした。

図 38.ダイレクトメールで送付した勧誘チラシ

- セミナー

デジタルハーツで主催した事業説明会のほか、IPA が主催するセキュリティセミナー（9/5 開催）、宮城県損害保険代理業協会が主催するセミナー（9/25 開催）にて、名刺交換やアンケートにて入手した連絡先に連絡をする形で勧誘活動を行った。

- その他

東北経済産業局に手配いただき、河北新報に記事を掲載いただいた。

河北新報
概要：主に宮城県を中心とした東北地方のブロック紙
発行部数：約 43 万部（宮城県）
世帯普及率：43.87%（宮城県）
推定読者数：約 113 万人（宮城県）※宮城県の世帯数は約 99 万世帯、人口は約 231 万人

また、経済産業省及び損保ジャパンの協力を得て、地方銀行、大手自動車系、大手製紙会社系のサプライチェーン企業へのアプローチを試みたが、具体的な実証参加企業獲得には至らなかった。地域電力会社にも 10/10 に協力依頼を行い、快諾を得たが、10/12 に上陸した台風 19 号の影響により実証参加企業の開拓等の協力を得ることはできなかった。

3-5-2. 実証参加企業の獲得結果

開始当初は地場経済団体へ協力を仰ぎ、その会員企業への参加募集を主軸として考えていたが、団体によってサイバーセキュリティに対する意識が大きく異なる状況や、団体の意識が高くても会員企業側の同意が得られにくい状況が発生し、見込んでいた参加募集数に届かない状況が続いた。

特に宮城県中小企業団体中央会、協同組合仙台卸商センター、仙台自動車整備工業団地協同組合、一般社団法人みやぎ工業会については、いずれも本事業への関心が高く速やかに個別企業を紹介してくれ、紹介された企業側もこれら団体の紹介ならばと非常に前向きであったため、こうした団体の紹介案件で多数の獲得が見込めたが、その後訪問設置の日程調整がなかなか進まないことや、ネットワーク環境の問題による撤去等があり、機器設置に難航した。

このため、特に９月以降、自社ポータルサイト、IPA サイト、IPA を経由して地場大企業からのサプライチェーンアプローチ、損保ジャパンの関与企業への声がけ、地場企業が持つ顧客企業への声がけ、ダイレクトメールによる募集及び自社関与企業への声がけなど複数の手段にて参加募集を集中して行い、実証参加企業の獲得を進めた結果、11 月に目標とする実証参加企業を獲得することができた。東北エリアでのデジタルハーツの認知度の低さを埋め合わせする形で地場企業に活動してもらうことにより多くの接点を確保し、また事業自体の信頼性与えることで参加申込みを増やすことができた(表 6,図 39)。

なお、セミナーに関しては、東北エリアにおいてのデジタルハーツの知名度の低さ、既存顧客の少なさからセミナー自体の集客、セミナー参加企業からの獲得も非常に難航した。ダイレクトメールからの参加獲得も非常に難しいと予測していたが、経済産業省及び IPA 連名による事業説明の書面とともに発出したことで、信用が増し、多数の獲得を得ることができた。

	アプローチ	申込み		機器設置		
	企業数	企業数	申込み率	企業数	設置率	構成比
自社及び地場企業での開拓	55	49	89.1%	40	81.6%	49.4%
地域団体からの紹介	110	29	26.4%	17	58.6%	21.0%
ダイレクトメール	99,500	19	1.9%	13	68.4%	16.0%
セミナー	77	14	18.2%	11	78.6%	13.6%
合計		111	–	81	73.0%	100.0%

表 6.獲得手段別の企業数

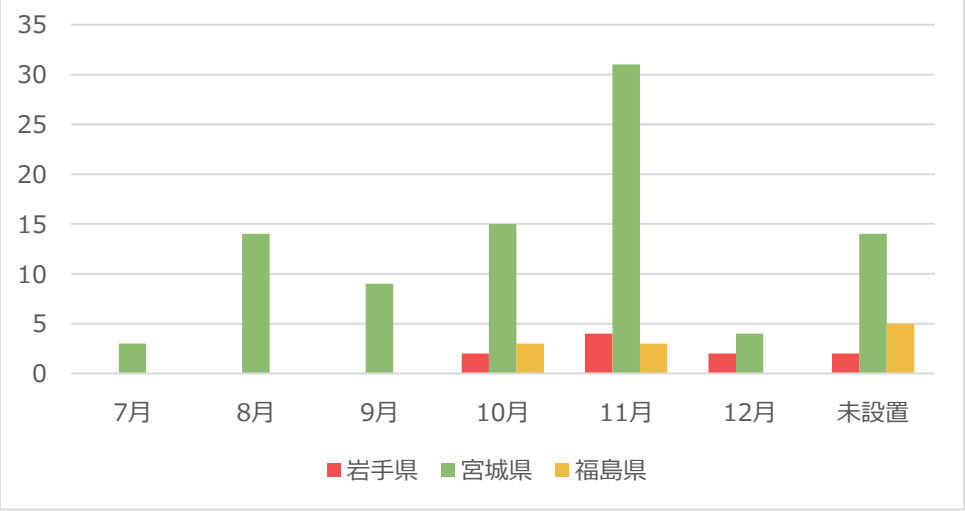


図 39. 設置月と設置場所ごとの件数推移

3-5-3. *SECURITY ACTION* の啓蒙

お助け隊事業を通して SECURITY ACTION の説明等の促進活動を行った企業数は、147 社となった。このうち、星を獲得した企業数は以下のとおりとなった。

・一つ星を獲得した企業数 15 社
・二つ星を獲得した企業数 8 社

SECURITY ACTION の主な啓蒙方法は、事業説明会・各報告会での紹介、各企業への事業内容説明訪問時・設置作業訪問時に IPA パンフレットを持参して説明する形にて行った。

その際に挙がった質問や反応としては、具体的メリットや活用方法についての内容であった。現状ではあくまで自己申告制の対外的なアピール手段ではあるものの、制度自体の認知度が低く、サプライチェーンの観点からも SECURITY ACTION を導入推奨されるようなケースはなかったことから、導入メリットを感じさせることが困難であった。

SECURITY ACTION は中小企業のセキュリティレベルを上げるための施策であると理解しているものの、制度説明の際に SECURITY ACTION に登録してもらうこと自体が目的となってしまうケースがあるため、メリット、他認証システムとの違いを再度整理した上で、セキュリティ向上のための手段であることを啓発している必要性があると考えられる。

3-5-4. 実証参加企業プロファイル

実証参加企業のプロファイル構成は以下のとおりである（合計 111 社）。

状態の説明

設置 NG：申込みはあったものの、何らかの理由でセンサー機器の設置に至らず参加を辞退した企業
設置完了：センサー機器の設置が完了し実証を開始した企業
撤去：一度は設置完了に至ったものの、何らかの理由にてセンサー機器を撤去し、監視を中断した企業

- 業種の構成

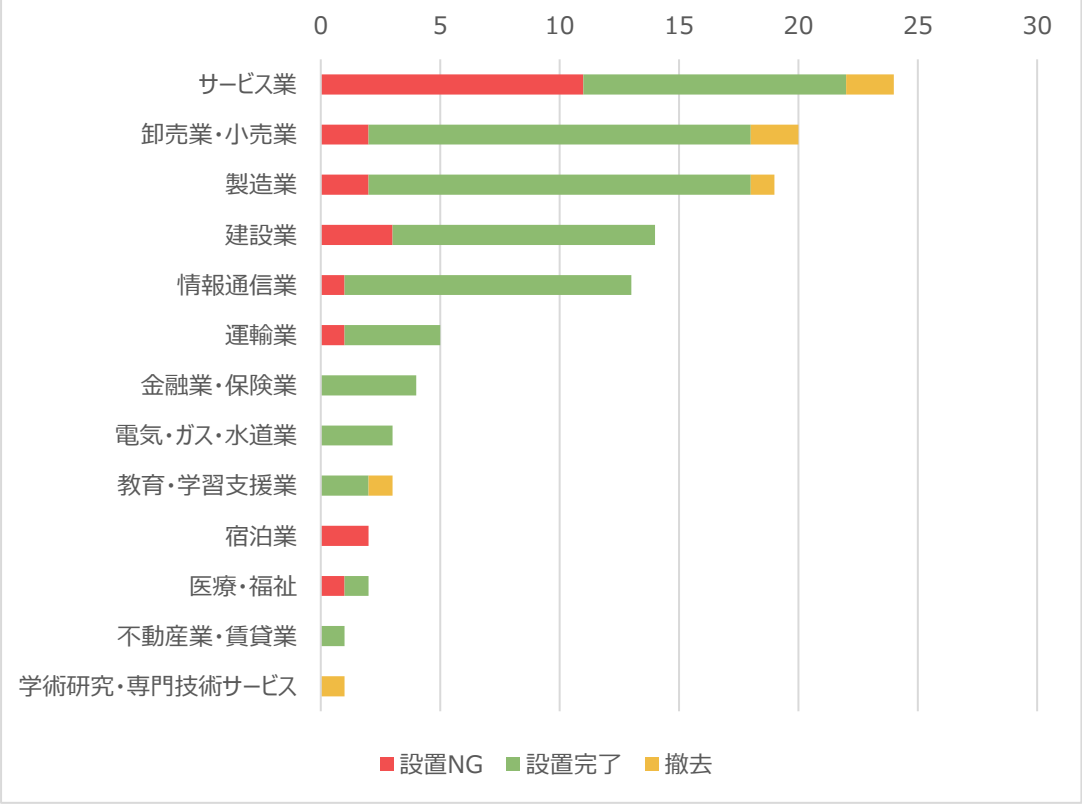


図 40.実証参加企業の業種別構成

ダイレクトメールの配信先として、サイバーセキュリティに意識が高いと思われる業種を選定したことも影響していると思われるが、選定した業種が上位に並ぶ結果となった(図 40)。サービス業の設置 NG となった件数が特筆して多いが、そのうちの約半数が IT 系サービス事業者であり、特殊な IT 環境に依存する要因で設置 NG となったことが想定される。

想定より参加が少なかった業種としては宿泊業で、サイバーセキュリティに対しての意識・リテラシーの問題なのか既に何らかの対策がなされているかについては今後調査をしていく必要がある。

- 従業員数の構成

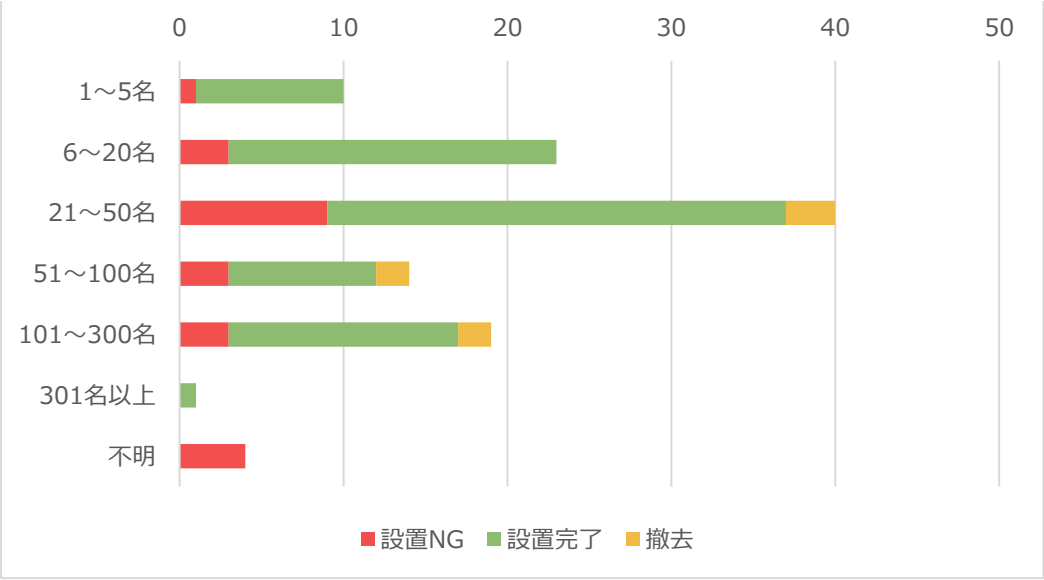


図 41.実証参加企業の従業員数の構成

- 資本金の構成

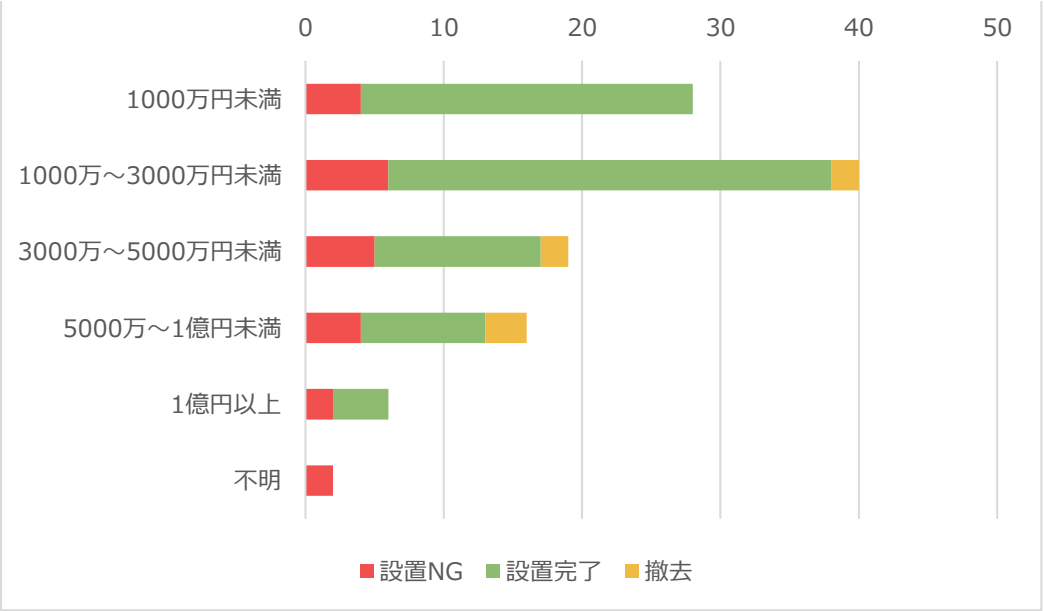


図 42.実証参加企業の資本金の構成

- 実証参加企業エリアの分布

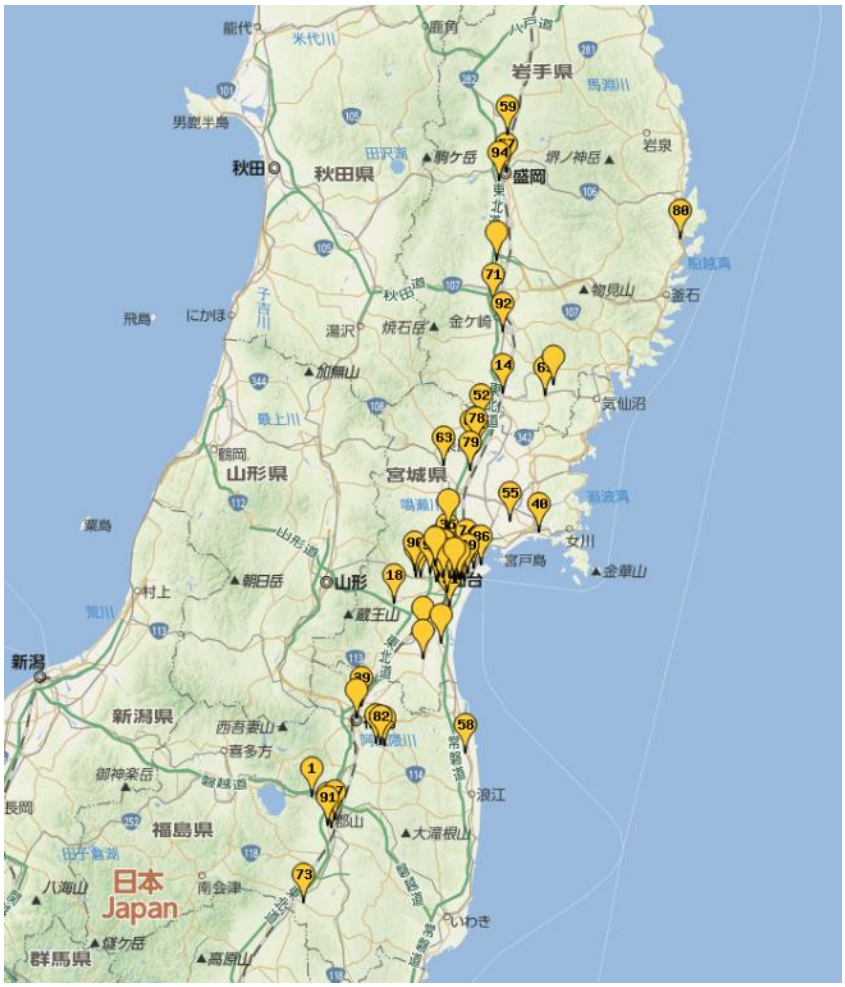


図 43.実証参加企業のエリア分布

実証参加企業 111 社
　宮城県 90 社
　岩手県 10 件
　福島県 11 件

3-5-5. 機器設置 *NG*・撤去企業について

実証への参加申込みがあったが機器設置に至らなかったケース、または機器を撤去したケースは下記となる。なお、機器設置 NG・撤去企業においても、サイバーセキュリティ情報の発信や、各報告会への参加勧誘は継続的に実施した。

- 設置前（設置作業時含む）に機器設置に至らなかったケース（23 件）

・ネットワークセンサーで取得したログデータを Starlight へログ送信を行うために、ファイアウォールのいくつかのネットワークポートを用途に応じて通信許可をする必要がある。ネットワーク管理業者などにてネットワーク管理を委託している場合、その作業を管理上、またはセキュリティ上の理由などにより実施いただけず、設置に至らなかった。

・台風被災のため、自社内対応または関与先対応などに追われることとなり、設置自体を見送りとした。

・機器設置時に回線速度テストを実施し、設置前と設置後に明らかな回線速度低下が見受けられたため、状態を切り戻し、設置を見送りとした。

・設置日程調整段階で、申込み企業と何度か連絡を試みるも連絡が取れなくなってしまった。

・親会社からの何らかの理由で設置許可が下りず、導入を断念した。

・設置期限間際（12 月末）のお申込みで、事務所引っ越しを 1 月上旬に控えていたため、設置期限に間に合わず、設置を断念した。

・設置にうかがった際、ネットワーク構成上、監視機器を導入することができないネットワーク構成であった。

※導入できないネットワーク構成例：無線アクセスポイント内蔵ルータを利用しており、社内 LAN をすべて無線 LAN で行っている場合(図 44)

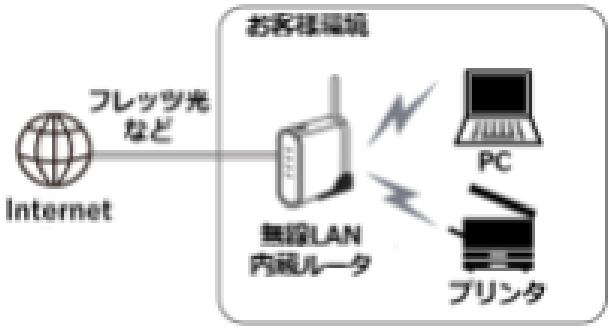


図 44.導入できないネットワーク構成例

- 設置後に監視機器を撤去したケース（７件）

  ・業務繁忙時間にてインターネット速度が低下し、業務に支障が出たため撤去した。（５件）

  ・特定の業務アプリケーションを使用した際、レスポンスが極端に低下したため撤去した。（１件）

  ・構内 IP 電話を使用した際、会話切断が発生し、業務影響があるとして撤去した。（１件）

設置における今後の改善点としては、３点ある。

１点目は、回線速度の詳細確認を行うことで、設置前、設置後の速度確認はもとより、月末月初などの業務繁忙期と思われる時間帯や始業直後など、通信が頻繁に行われる時間帯の速度チェックを行うことで、導入後の回線速度遅延の変化の見極めが可能となる。

２点目は、導入前にネットワーク構成を事前に把握しておくことで、設置に行ったがネットワーク構成上の理由で設置を取りやめることを防ぐことである。ただし、これを行うことは導入までの確認工数が増え、かかる人員やコストの増大となる可能性がある。

３点目は、導入設置時に設置人員がネットワーク構成や配線状況をドキュメント化しておくことである。万が一監視機器を取り外す状況となった際、電話等リモートで対応が行えるようにするためである。

４．ビジネス化に向けた課題・検討

４-１．実証参加企業向けアンケートの結果

実証事業への感想、セキュリティに関する意識、今後のサービス化に向けた意見調査のため、実証参加企業向けにアンケートを実施した（n=40）。

アンケート回答期間：2020 年 1 月 15 日（水）～2020 年 1 月 29 日（水）

（Q１）サイバーセキュリティ対策・導入状況について

Q1-1.セキュリティ製品・サービスの導入状況についてお答えください。

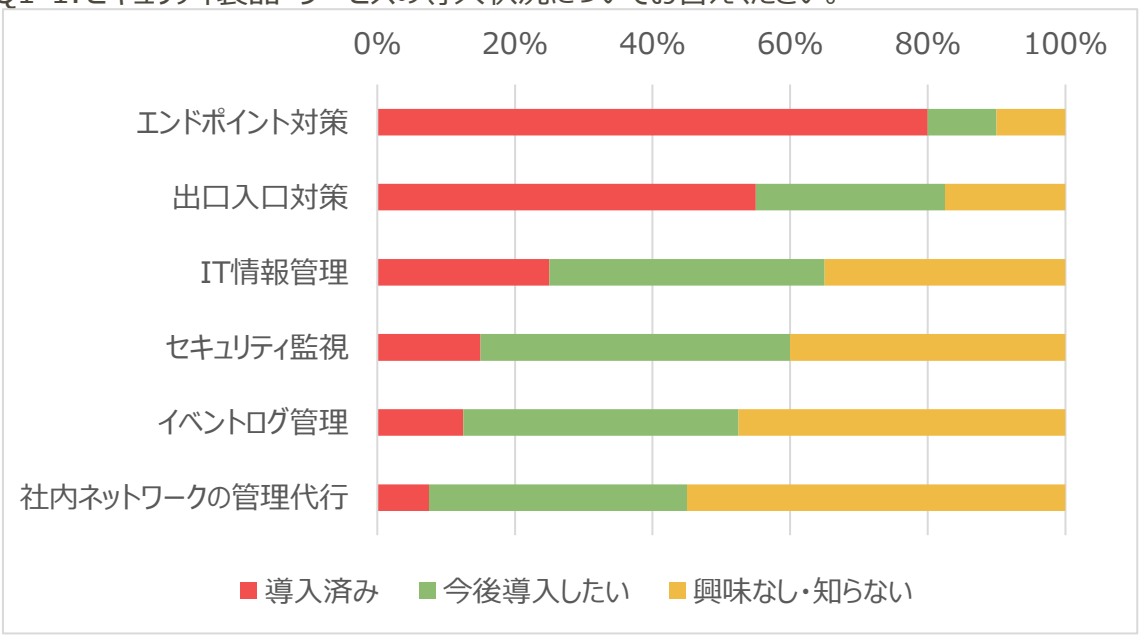


図 45.Q1-1 の回答集計

考察：多数の企業においてエンドポイント対策（アンチウィルス対策ソフトのインストール等）を実施済みであることが分かった。セキュリティ監視、イベントログ監視、社内ネットワークの管理代行を導入済みの企業は 20%以下にとどまった。アンチウィルスソフトは既によく知られており、安価なものがあるのに対して、セキュリティサービスは必要性、効果、価格などが分かりにくく、導入が進んでいないことがうかがえる。

Q1-2.情報セキュリティ対策状況についてお答えください。

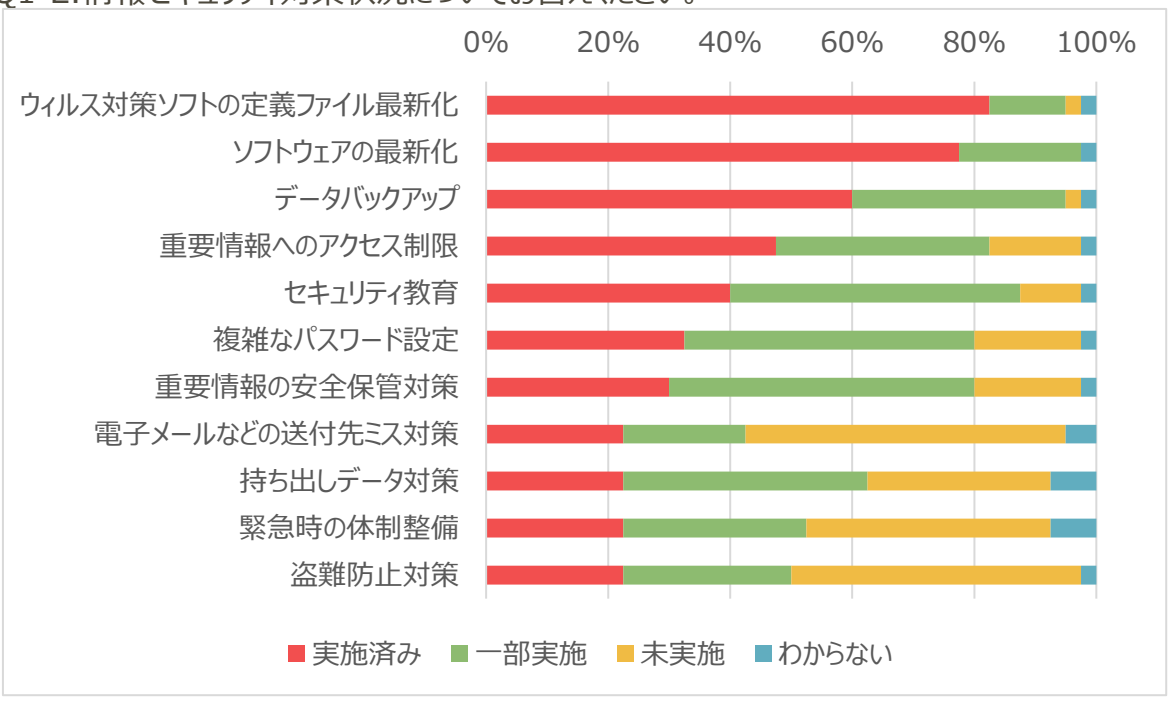


図 46.Q1-2 の回答集計

考察：ウィルス対策ソフトの最新化やデータのバックアップ等への意識はある一方で、教育や社内ポリシー策定などのソフト面の対応が不十分であることが分かった。これらの対策の多くはそれほどお金をかけなくてもできるものであって、外部からのサイバー攻撃及び内部からの情報漏洩に大きな効果が期待されるものであり、専門家を交え、社内のセキュリティ対策を構築することが強く求められている。

Q1-3.セキュリティサービスを導入するにあたり障壁となっているものは何ですか？（複数回答）

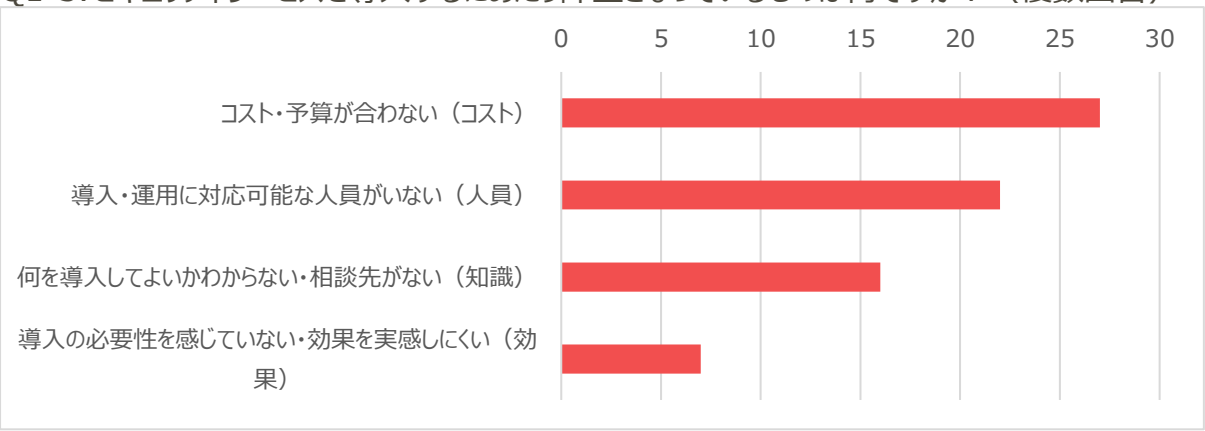


図 47.Q1-3 の回答集計

考察：セキュリティに関してはコストや人員の問題が障壁となっていることが分かった。また、導入のための人員や知識も不足しており、なかなか対策が進んでいないことが分かった。

Q1-4.サイバーセキュリティ対策に年間どれくらいの経費をかけていますか？

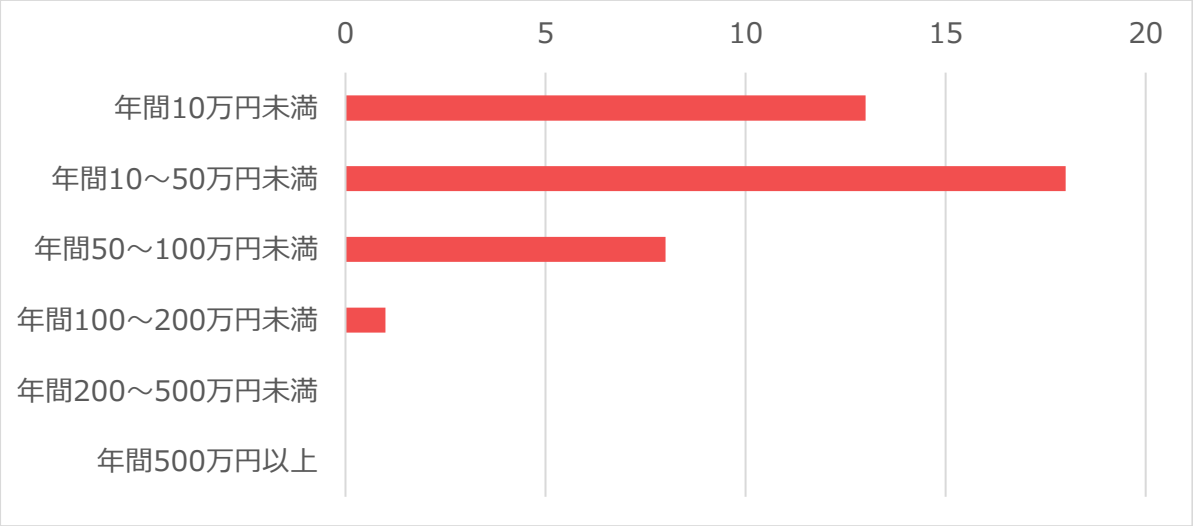


図 48.Q1-4 の回答集計

考察：サイバーセキュリティにかけている経費は年間 50 万円未満と少ないことが分かった。

Q1-5.自社のサイバーセキュリティについて

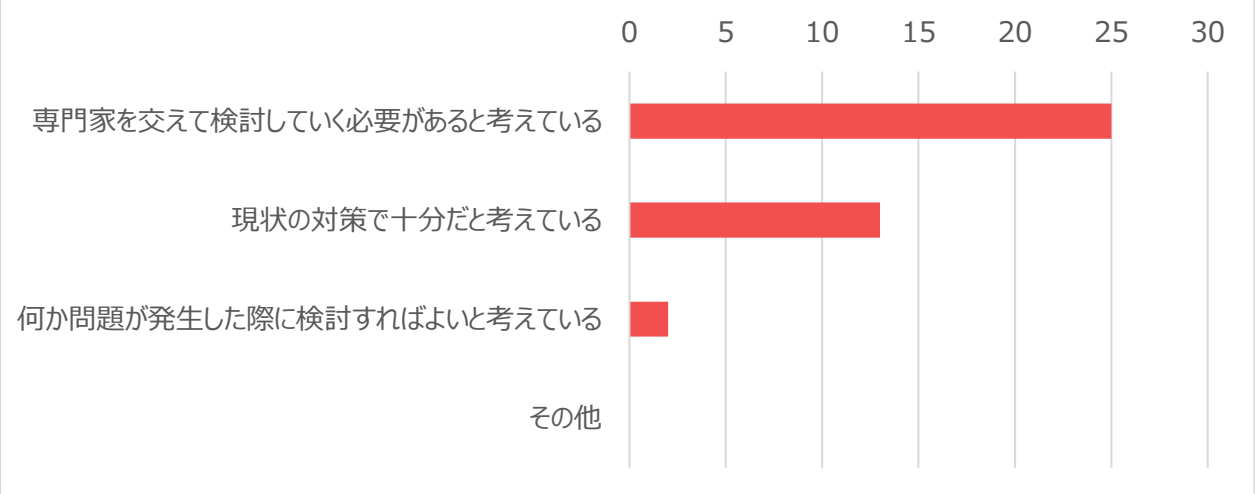


図 49.Q1-5 の回答集計

考察：自社のサイバーセキュリティ対策について、専門家を交えて検討したいという企業が多かった。他の回答結果も踏まえれば、まず専門家を交えて社員教育等の現状でも可能な対策をしっかりと講じた上で、さらなる対策に必要なコストと効果を勘案し、自社に必要なサイバーセキュリティ対策を進めていく上では、まず自社の現状をよく理解し寄り添った形で相談できる専門家が必要であると考えられる。

Q1-6.現状の社内 IT 環境を運用する人員について最も近いものは何ですか？

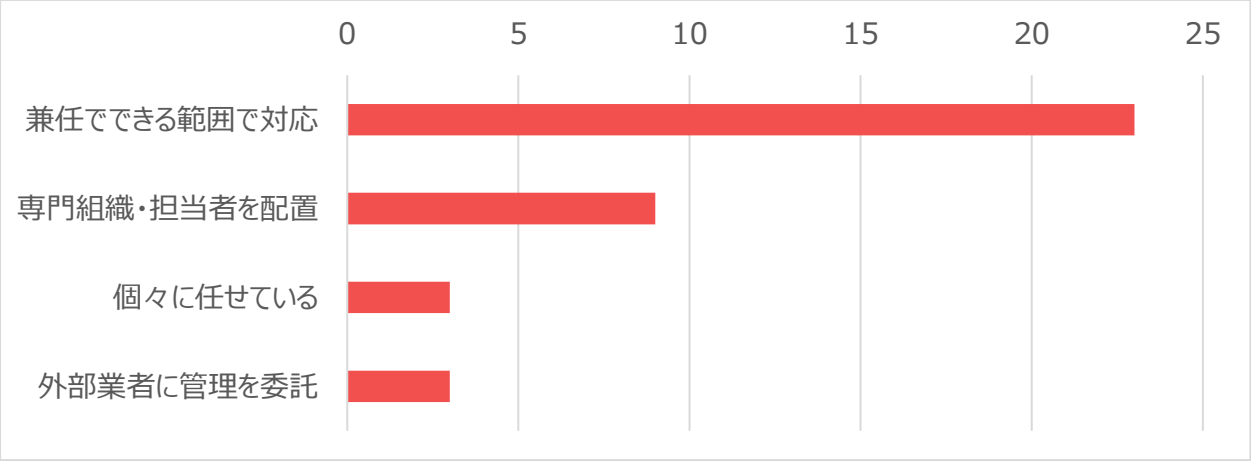


図 50.Q1-6 の回答集計

考察：IT 運用は兼務で対応している企業が多数であり、専門組織・担当者を配置していたり、外部業者に管理を委託していたりしている企業はごく少数であった。

Q1-7.SECURITY ACTION の取得状況について

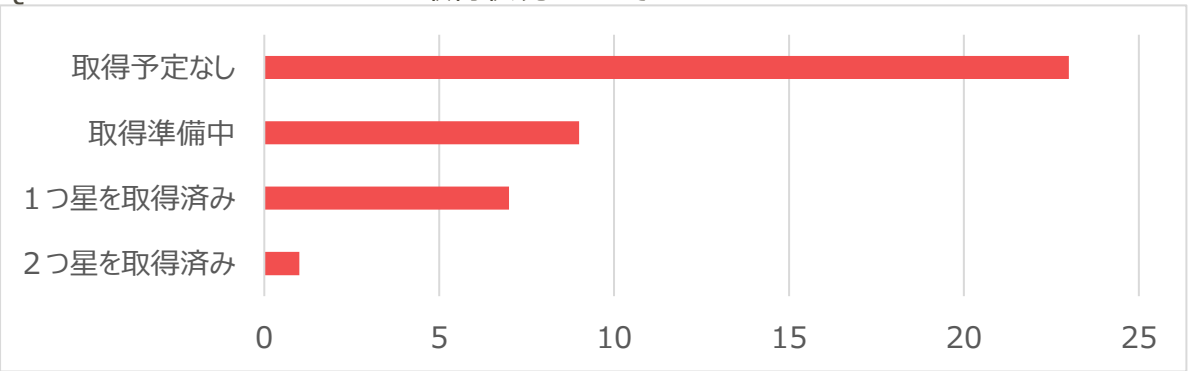


図 51.Q1-7 の回答集計

考察：兼務であり、ソフト面の対応への意識が薄いためか、SECURITY ACTION の取得に前向きな企業は少なかった。取得によるメリットを感じておらず、すぐできる対策についても優先度が低くなかなか進んでいない現実が浮き彫りとなった。

（Q2）サイバーセキュリティお助け隊について

Q2-1.参加動機は何ですか？（複数回答）

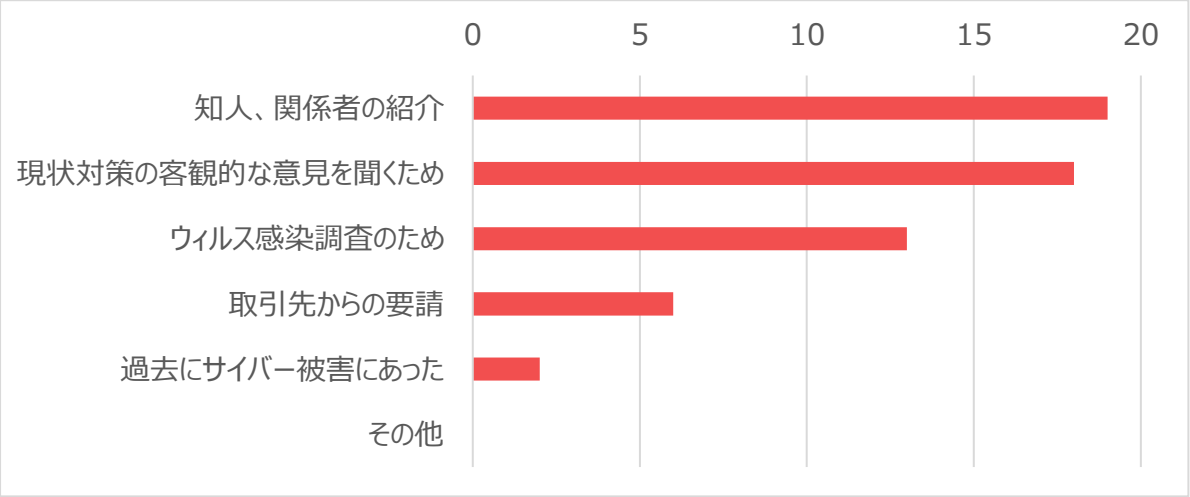


図 52.Q2-1 の回答集計

考察：最多数が知人・関係者の紹介であり、信頼して任せられる中小企業向けセキュリティサービスが存在しない現状がうかがえた。また、現状に対する客観的な意見を聞きたいというニーズも高かった。一方で取引先からの要請や過去にサイバー被害に遭ったという企業は少なく、まだサイバー攻撃は身近なリスクと認識されていない現状がうかがえた。

Q2-2.今回のサイバーセキュリティお助け隊のサービスが有料になった場合、妥当と思われる月額費用はいくらくらいだと思いますか？

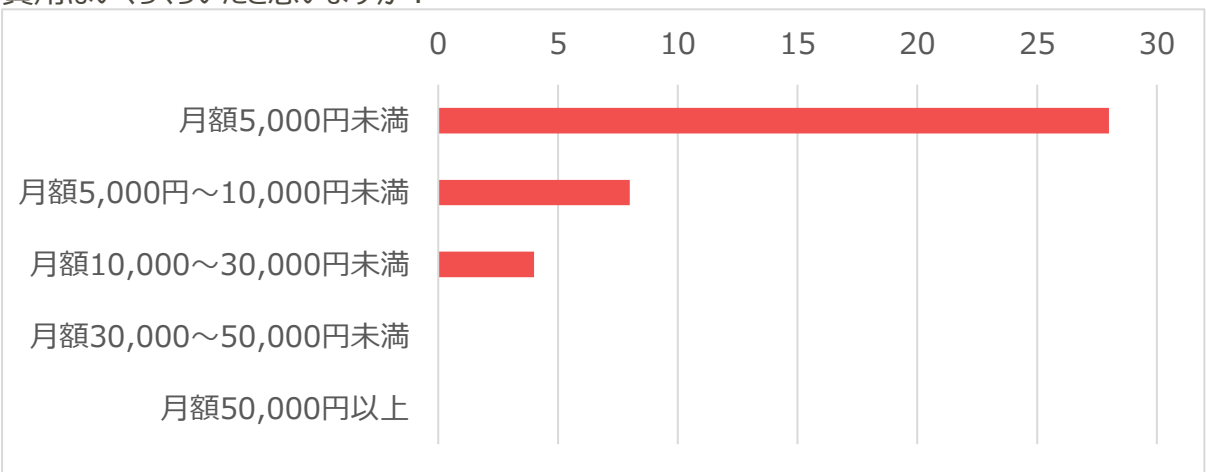


図 53.Q2-2 の回答集計

考察：かけられる費用は月額 5000 円未満と非常に少なく、対策を講じることの経済的メリットを認識してもらうには至らなかった。

Q2-3.今後、サイバーセキュリティお助け隊が継続または再開される場合、参加したいと思いますか？

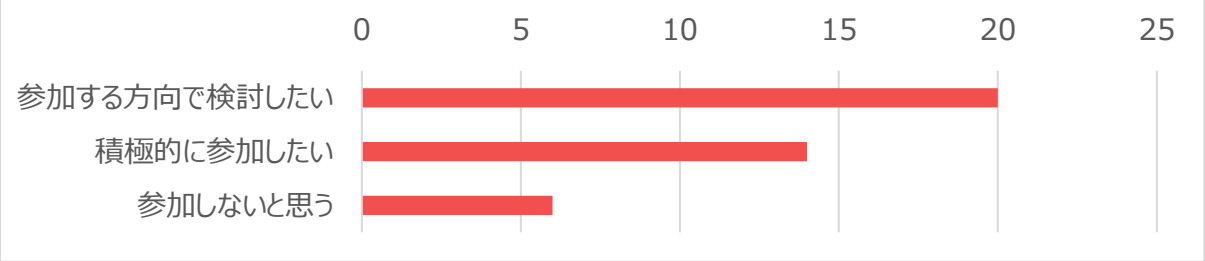


図 54.Q2-3 の回答集計

考察：多数の企業から今後も参加したいという声があった。

Q2-4.サイバーセキュリティお助け隊に参加して、社内でサイバー対策についての意識は高まりましたか？

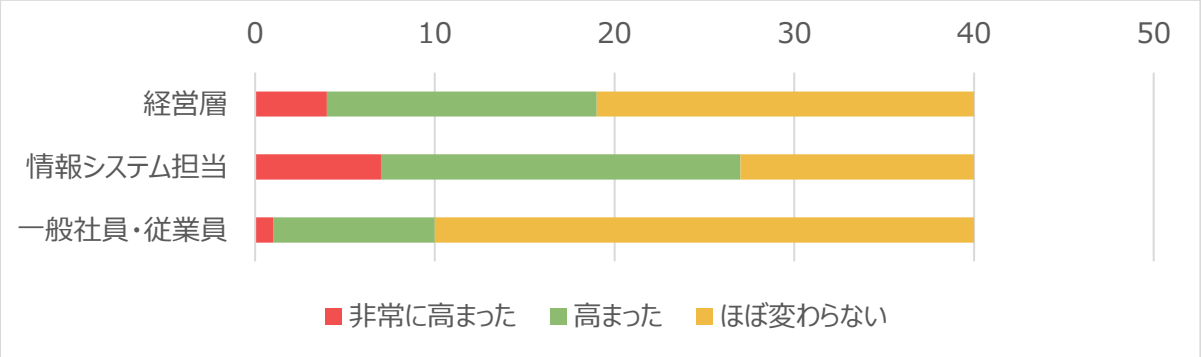


図 55.Q2-4 の回答集計

考察：情報システム部門の方の過半数はサイバー対策への意識が高まった反面、経営層や一般社員への浸透は不十分な結果となった。

（Q3）サイバー保険について

Q3-1.サイバー保険に加入していますか？存在を知っていますか？

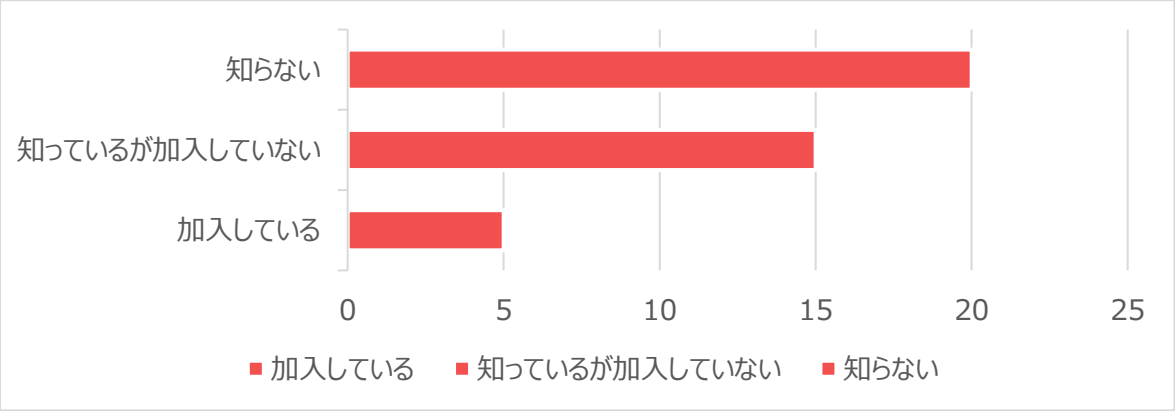


図 56.Q3-1 の回答集計

考察：サイバー保険を知らないという回答が多数を占めた一方、加入している企業も一部存在した。

Q3-2.サイバー保険に加入した理由は何ですか？（複数回答）
※Q3-1 でサイバー保険を「加入している」と回答した企業への質問

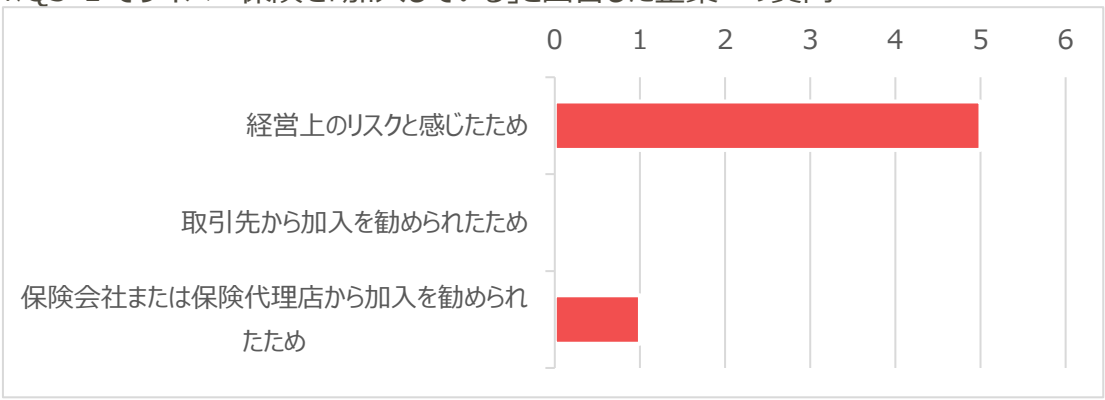


図 57.Q3-2 の回答集計

考察：加入している企業はすべて取引先や保険会社からの勧誘ではなく、経営上のリスクから加入していた。

Q3-3.サイバー保険に加入していない理由は何ですか？
※Q3-1 でサイバー保険を「知っているが加入していない」と回答した企業への質問

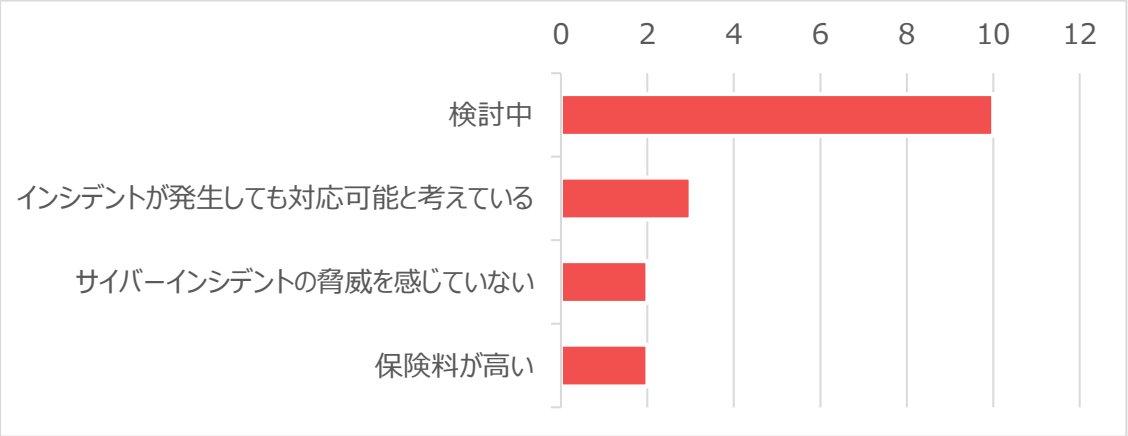


図 58.Q3-3 の回答集計

考察：知っているが加入していない企業は、具体的な回答が少なく、そもそもコストやメリットについての具体的な理解が進んでいるとはいえない状況がうかがえた。

Q3-4.サイバー保険の補償として必要と感じるものは何ですか？（複数回答）

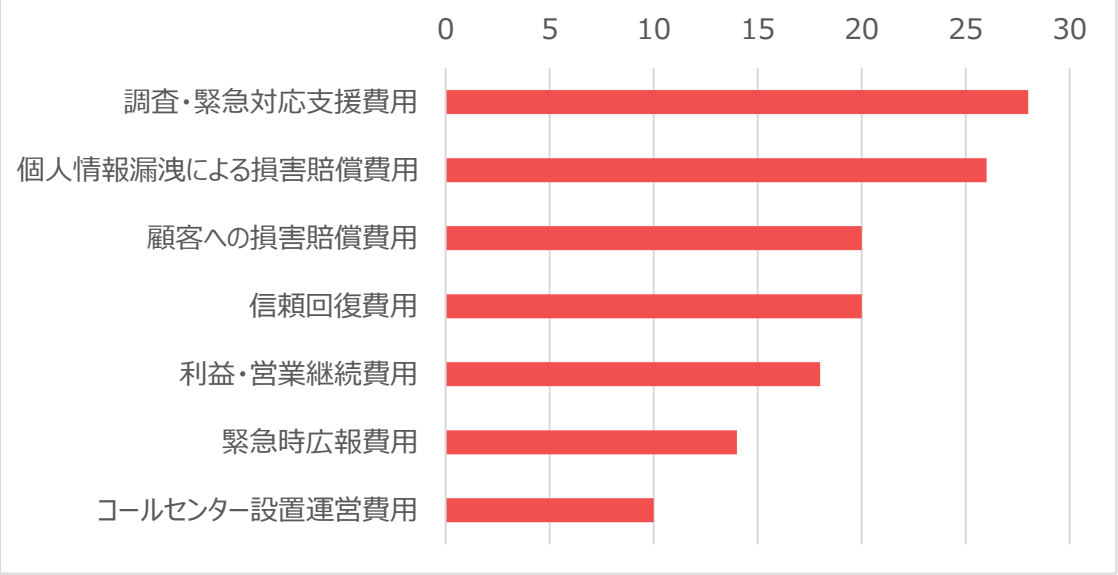


図 59.Q3-4 の回答集計

考察：調査対応費用や各種賠償費用を求める声が多数を占めた。一方、広報やコールセンター等の費用まで必要と考える企業は比較的少なかった。

Q3-5.サイバー保険の加入を検討する年間の予算感は？

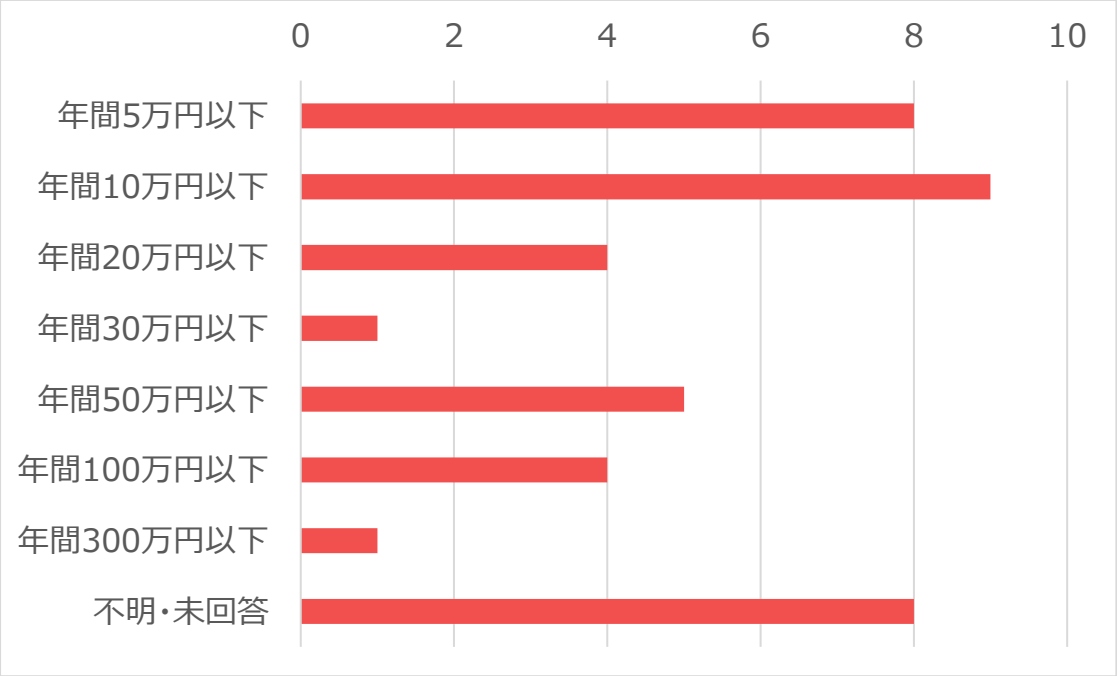


図 60.Q3-5 の回答集計

考察：年間 10 万円以下の回答が多数を占めた。一方で分布は正規分布にはならず、年間５０万円以下とする企業も比較的多数を占めた。これは、そもそもサイバー保険のメリットを理解しない層としては 10 万円程度、被害に遭った場合の対応を考えると 50 万円程度と考える層に分かれたものと考えられる。

４-２．中小企業のセキュリティ対策の課題とビジネス化に向けた検討

以下のとおり、今回の実証を通じて得られた現状を整理した上で、それぞれから見えてきた課題に対応する形でビジネス化に向けて必要な要素について検討を行った。

（１）現状把握・可視化

【現状整理】

今回の事業では、顧客のネットワークにできるだけ影響を及ぼさないようなソリューションを用意し、ネットワーク監視による可視化を試みたが、それでも一部の企業において監視機器の導入を断念する事例があった。その背景として、社内のネットワークや PC 等のネットワーク機器を管理する専任の IT 管理者が不在であり、社長や総務担当が兼務して知識が不足するままに対応しているため、ネットワーク構成が把握できていない、または外部の業者に委託していてブラックボックス化しているという状況があった。多くの中小企業では、帯域保証や固定 IP を持たないインターネット接続サービスを利用している実態があり、ネットワーク構成図を作成・把握している企業は全体の２～３割程度であった。

このためネットワークセンサー設置に伴う影響を事前に把握しきれず、また不具合と思われる事象が発生した場合の対応について十分な検討を行えないまま、少しでも異常があるなら機器設置を断念するという事態に至った事例があった。また、ネットワークセンサーの設置のために訪問した際、従業員の PC にパスワードが設定されていないことを確認し、適切に対応すべき旨の助言を行った事例があった。

ネットワーク構成の把握は、UTM やファイアウォールルータの導入には必須であり、サイバーセキュリティインシデントが疑われる事象が発生した場合の問題の切り分け等にも必要な情報となるものであり、こうした情報が書面化され把握している人材が社内にいないということが、今回の実証によって浮き彫りになった最も大きな課題であった。

【ビジネス化検討】

多くの中小企業の現状は、ネットワークセンサーの設置などハードウェアの導入以前の状況に置かれていることを踏まえ、必要な支援策としてはまず、ネットワーク構成を書面に落として現状を把握することや、OS やセキュリティソフトのバージョンを最新にする等の基礎的な対応を伴走する支援が求められている。

仮に「情報セキュリティ５か条」を実施する状況においても、担当者レベルで実施する意義は理解できても、いざ実施するとなると一定の知識、リソースは必要となってくる。これを充当するためには、中堅企業以上の情報システム部門の経験者を採用するか、社内の人材を育てていくかの選択になるが、いずれも中小企業にとっては経験者採用費・人件費などの負担、教育実施の時間・コスト捻出などの課題が多く現実的な対策とはならないため、情報システム部門のアウトソースサービスなどを利用すべきである。

例えばデジタルハーツでは、IT 機器の資産管理、構築、運用を行う情報システム部門のアウトソーシング事業（情シスサポート君）を提供しているが、こうした広い意味での IT サポートが、企業のサイバーセキュリティ対策の底上げにつながることが期待される。

また、対象企業のほぼすべてで社内に外部向けのサーバ等が設置されておらず外部から内部へのアクセスが不要であること等を背景に、UTM を導入している企業が少なかったが、本実証のアラート分析にて UTM の導入有無によってアラート発報数は１． ５倍以上となっていたことからも、サイバーインシデントのリスク低減に貢献する UTM の導入を積極的に推奨していくべきだと考える。

（２）サイバーセキュリティ対策のコスト意識向上

【現状整理】

アンケート結果に代表されるように、今回の実証で接した企業の多くからはサイバーセキュリティ対策にそれほど多くの予算をかけることはできないという声が圧倒的多数であった。今回の実証も無料であるということで参加した企業が多数を占めた。

そもそもサイバーセキュリティ対策は、企業において直接的な売上げ・利益に貢献する活動ではなく、サイバーセキュリティ対策の効果の不透明さも相まって、セキュリティベンダーが提供するセキュリティサービスを導入可能なまでの予算化がされていない状況が見受けられる。

アンケート結果では年間 200 万円以上の予算をかけている企業は 0 社で、年間予算 10 万円～50 万円未満の企業が最も多く、セキュリティ対策にかけられている予算と、必要な対策を実施するための予算に乖離が生じていることが見受けられる。また、これらの対策はあくまで最低限の対策であり、各企業・各業種に応じた追加対策費用は更に必要となる。

対策予算が少ないのは、収益上コスト捻出できないのか、コストをかける必要がないという判断によるものなのかは定かではないが、アンケートや報告会での質疑を参照する限りでは、漠然とセキュリティ対策をしなければならないことは理解しているが、具体的に何をしてよいか分からないため予算化するかの議論にも至っていないというのが実情であると想定する。また、東北エリアの経済状態を参照する限り、セキュリティ対策にかけるコストを最優先で捻出できる状態でないことも理解はできる。

中小企業のサイバーセキュリティは実害が発生してからでないとその重要性に気付くことがないため、多くの中小企業において対応は後手となってしまう状況がある。リスクアセスメントを行うことにより深刻な危機を想定しそれに対応することでリスクヘッジできることがセキュリティ対策の効果であると考え、それを啓蒙していく必要がある。

一方で最低限必要な対策は、SECURITY ACTION で掲げられている「情報セキュリティ 5 か条」であり、それに対するソリューションとして、ウィルス対策ソフトの導入や、UTM の導入が考えられる。Windows に標準搭載する Windows Defender によりウィルス対策ソフトの導入はほぼ浸透できているものの、UTM やファイアウォールの導入率はアンケート結果からも分かるとおりまだ５０％程度である。ただし、当事業に参加している企業はサイバーセキュリティに対する意識が高めの企業群であるため、実態としては全体として５０％を大きく割ることも想定できる。

【ビジネス化検討】

企業においてどういったサイバーリスクがあるのかが把握されていないままセキュリティ対策を導入することは考えにくい。中小企業がまず行うことはリスクアセスメントであり、それを以て企業内のセキュリティ意識を高め、対策を打つ必要がある。

サイバーセキュリティ自体は利益の拡大に資する取組みではないため、こうした投資は優先順位が低く位置づけられることから、進まない現状があることを踏まえ、サイバーセキュリティ対策を積極的に行うことでサプライチェーンから評価され売上げ拡大につながるという期待の情勢や、仮に被害に遭った場合の負の影響を同規模の企業の事例などから実感できる情報があることで、経営者の適切な投資判断を引き出せると考えられる。

その上で、比較的効果がわ分かりやすく、かつ業種や企業形態に依存しない UTM やその拡張サービスを安価に提供できるサービスを企業の実情に応じて選択できるようパッケージ化する等の工夫が必要と考えられる。

例えばデジタルハーツでは、顧客が運用するシステム・サービスに対する脆弱性診断を実施しているが、こうした現状把握を一度実施することで、自社が被害を受ける可能性がある領域がどのあたりにあるのかを知ることは対策予算を考える上で有益なものとなると考えられる。

（３）十分な選択肢の提示

【現状整理】

当実証に参加した企業の参加動機は「自社のセキュリティ対策について、専門家を交えて検討していく必要がある」が大多数であった。本実証事業の参加企業獲得及び機器設置等の対応に際して、地場 IT ベンダーとの協力体制を構築したが、コピー機や複合機などをメインで扱う事務器系 IT ベンダー、もしくはソフトウェア開発やクラウドサービスなどを展開する開発系 IT ベンダー、電話・通信回線等を扱う通信系 IT ベンダーは多いものの、セキュリティサービスを積極的に扱う IT ベンダーが少ない印象を受けた。もちろんそういった企業においても中小企業の企業内環境に精通しており、そのアドバンテージを生かしてセキュリティサービスを導入している例もあるが、偏った取扱いメーカー、偏ったサービスのみを提供している状況も推測できる。

【ビジネス化検討】

中小企業がそれぞれ置かれた課題に対して、適切なソリューション、適切なサービス、適切な対策案を提供するためには、できるだけフラットな立場で直接相談できる組織か、もしくは各 IT ベンダーのバックサポートとして専門的な情報提供が可能な組織が必要である。現状では、IPA が運営する「登録セキスペ」や「情報セキュリティ安心窓口」が考えられるが、具体的なサービス紹介や具体的な相談先の紹介ができる、認定サービスや認定企業を設けて中小企業をスムーズに誘導できる体制が必要だと考える。その際、一部の企業が排他的・独占的に行うのではなく、オープンな形で情報提供し、事業者がそれぞれのニーズに応じて適切に選択できることが望ましい。

（４）サービスを担う専門人材育成

【現状整理】

今回の実証でお助け隊に従事した人材のうち、SOC アナリストとしてアラートの分析を行った者は情報処理安全確保支援士の有資格者を中心とした高度な専門人材であったが、ネットワークセンサーの設置や、アラートのレポート作成などについてはそこまで高度なスキルが求められない。実際、資格を持たず経験の浅い社内人材や、サイバーセキュリティを主たる事業としない地場 IT ベンダーを中心にセンサー設置を行ったが、知識不足によるトラブル等は生じなかった。インシデント対応に際しても、現地でのログ分析等により詳細把握まで行うことは難しかったが、遠隔による高度専門家からの助言や、データを持ち帰って専門的分析を実施する等により、必要な技術的支援を行うことができた。

【ビジネス化検討】

中小企業向けに安価なサービス提供を行うためには、可能な限り高度人材の関与を効率化して生産性を高める必要がある。今回の実証ではアラート分析を AI 導入により効率化し、平時のレポート提供も最大限効率化することができた。一方で中小企業にサービスの満足度を高めてもらうためには丁寧な接点構築が必要であり、こうした領域については、高い専門性がなくてもよいので気軽に相談できる体制を構築する必要がある。

こうしたサービスを担う人材スキル像としては、必ずしも高い専門性・資格を有している必要はないが、PC やシステムに対する一定の知識を有した上で、顧客に寄り添い、専門的な内容に関しては適宜専門家に確認する等の体制を構築することで対応が可能である。

（５）地域での持続的な啓蒙活動

【現状整理】

多くの中小企業はセキュリティ対策を講じる必要性を感じているものの、何をすべきか、誰に相談すべきかが分からない中で、特に保守的な東北地域では公的機関や地域経済団体等を通じた情報発信が有効だった。例えば、ダイレクトメール送付による集客の際、経済産業省及び IPA の連名による書面を同封したことで、信用が増し、実証参加企業の獲得につながった。実際、チラシを見た事業者からの電話問合せの中に、公的機関の紙も入っていたので売り込み等ではなく政府の実証企業だと理解したが、詳細を確認したいという内容があった。個別企業の開拓についても、仙台卸商センターのような経済団体が紹介してくれた企業からの加入が多く得られ、技術的な内容よりも誰が推進するものであるかということが東北地域では重視されていることが分かった。

また、2019 年 10 月後半以降 Emotet の感染事例が増加したが、こうした状況に応じて 11/28 にポータルサイト上で推奨対応を呼びかけたほか、12/11 に行った中間報告会では実際の感染事例に伴う対応について説明を行った。今後も、マルウェアの流行等の状況に即して適時適切な対応を呼びかけていくことが地域のサイバーセキュリティ対策の底上げにつながり、引いてはビジネス化に資するものと考えられた。2/6 に行った成果報告会においても、参加者から、地域の消防団のように、地元の人材が中心となって勉強会を行いながら、公的機関や専門家を交えた会合を重ねていきながら面的にサイバーセキュリティ対策を考えていきたいという声が上がった。今回の実証に参加した企業の経営者や担当者の一部は、問題意識が高く知識レベルも高い者が存在した。こうした地元の人材が中心となった地域のレベル底上げが求められている。

【ビジネス化検討】

サイバーセキュリティに関する啓発を行っていく上では、私企業の主催によるセミナーではなく、公的機関や地域内で活動する専門家を交えた会合を定期的に行うことで、中小企業経営者にサイバーセキュリティ対策を考えてもらう機会を持つことがビジネス化において重要となる。

また、サービス提供型の視点から見ても、個々の中小企業を点でとらえて営業を行い、サービス提供を行うことは非常に効率が悪く、特に東北のような他地域と比較して経済規模が小さい地方においては展開が進まないことが容易に想像される。一方で、一定のエリアに集約された複数企業に対して同等のサービスを提供することにより効率化、低価格化することが可能であり、工業団地・商業団地の組合員に対してサービス価格を提供することで、双方にメリットのあるサイバーセキュリティ対策を行うことが可能となる。

４-３. あるべき中小企業向けサイバー保険の姿についての検討

サイバー保険には、サイバー被害に伴う保険金の支払い機能だけではなく、調査・緊急対応、緊急時広報、コールセンター対応など緊急的に発生する業務を必要に応じてコーディネートする機能も含まれており、サイバーインシデントが発生した際には事業者にとって有益なものとなるが、平時におけるサイバー攻撃の監視まで行うものではない。このため、本実証のような実態の可視化と一体となり、被害発生時の経済面の補償及び事業復旧のための体制整備支援を行うことが求められている。また、平時から、いざ有事が発生した場合の被害を最小化するとともに、速やかな事業継続を目指すという観点では、ＢＣＰに近いものであり、自然災害等と同様に、保険も組み入れた対策を自社であらかじめ検討し、定期的な訓練・研修によりアップデートしていく必要がある。

一方、中小企業へのサイバー保険の導入が進まない大きな理由として、Q3-1 のとおりサイバー保険を知らないとのアンケート回答が大半となっていることから、まずは内容の周知を徹底する必要がある。今回の実証のような官民での政策情報の発信や、地場企業と連携した啓発活動を面的に行っていくことが有効であると考えられる。

その際、現時点においても一定金額をセキュリティ対策に使っていることがアンケート結果から読み取れるため、例えばセキュリティ商材に保険を付帯するなど効率的なセキュリティサービスの開発が望ましいと考えられる。

具体的には、中小企業の実態に寄り添った安価なサービス・保険として、以下の 2 とおりについて今後検討を深める必要がある。

①加入しやすい安価なサイバー保険の検討
②セキュリティ商材へのサイバー保険の付帯

サイバーセキュリティサービスの導入に際しての障壁は Q1-3 のとおり、「コスト・予算が合わない」ことが多数を占めており、中小企業にとって必要な補償に絞った安価で加入しやすいサイバー保険が必要であると考える。なお②商品付帯とする場合、製品、サービスの内容に即した補償内容であるため、中小企業にとって十分とは限らず、通常のサイバー保険との併せての加入を検討する必要がある。商品付帯は当該製品・サービスの普及とともに保険も普及することになるが、安価な商品の場合には企業にどう届けるかが問題となる。Q2-1 のとおり、「知人・関係者の紹介」が多数を占めており、地場団体、グループ会社などの企業群としての付保のように広くリーチできる方法も検討すべきと考えられる。

いずれにしても商品付帯の場合は限定された補償内容となるため、自社に必要な補償を検討して別途上乗せで①のような保険に加入する必要がある。Q1-4 のとおり、年間のセキュリティ対策にかける経費としては「年間１０～５０万円未満」が多くを占めており、限られた予算内でいかに合理的なセキュリティサービスを構築できるかがポイントとなる。

自社に最適なあり方を検討する過程でサイバーセキュリティに対するリテラシー向上が見込めると考えられる。

４-４. 具体的なサービス提供の仕組み及び実証終了後のサービス提供の可能性

本実証事業の成果を踏まえ、具体的なサービス提供の仕組みや実証終了後のサービス提供の可能性について考察を行った。

まず、中小企業には情報システムを担当する専任者がおらず兼務で対応していることから、できる限り分かりやすいパッケージとして提供する必要がある。まずは現状のネットワーク構成を書面化し、SECURITY ACTION の一つ星レベルの対応を徹底した上で、UTM の導入等の追加的な取組みに伴う費用対効果を整理するまでの対応が必要となることから、こうした検討を伴走型でサポートする業務を提供することが求められている。

その上で、実際にセキュリティ投資に踏み切るためには、セキュリティ強化に伴う自社の信頼性向上が取引拡大等にどの程度つながるのか、あるいはサイバーインシデントに伴う事業継続リスクをどの程度軽減できるかといったコスト・メリットの可視化が必要となる。こうした情報について、本実証事業で得られた知見等に基づき情報提供を行い、他の実証地域で提供されている中小企業サービスも含め、幅広い選択肢の中から自社にとって最適なサービスを選択していただくことが理想である。

サービス提供者の立場からは、サービス提供の仕組みを効率化する必要がある。本実証事業を通じて、サイバーインシデントであるかの判定やインシデント発生時の技術的・専門的な領域に関しては高い知識レベルが要求されるものの、その頻度は少なく、現状把握、機器設置、月次報告の作成と送付等の多くの業務は基本的な知識で足りる業務が大半を占めた。このため、デジタルハーツではサイバーセキュリティブートキャンプ研修によるテスター人材をセキュリティ人材として活用する方策を進めているところ、こうした人材をうまく活用することにより業務効率化に資すると考えられる。

また、効率化の観点からも、個別の中小企業に説明して営業活動を行うのではなく、地域の経済団体等との連携による団体割引のような仕組みが期待される。本実証事業への協力を得られた団体のうち、仙台卸商センターでは今後も見据えた協力への期待も寄せられているところ、こうした地域経済団体との連携により効率的なサービス提供が可能となると考えられる。その際、サービスに付帯した安価なサイバー保険を付保することにより万が一の補償を行うことも可能となる。

ただし、本実証事業では東北の地域特性への理解、AI を活用したセキュリティ監視ソリューションである Starlight を中小企業に導入する場合に生じる課題の把握、実証参加企業やセミナー参加企業の獲得方策ごとの費用対効果などへの理解を深めることができたが、実証参加企業の獲得に時間を要したこともあり、サイバーセキュリティサービスの具体的な内容、価格帯、必要な人員体制等まで検討を深めるには至らなかった。加えて、東北でのビジネスには信頼関係の情勢

が不可欠なところ、1 年に満たない実証事業では一過性のものとして見られ信頼獲得にはまだ課題が残った。こうしたことから、今後も引き続き継続的にウェブサイトによる情報発信やサイバーセキュリティに関する説明会等を継続していきながら、地域の信頼を得てサービスの具体的な内容を設計していく必要がある。

以上